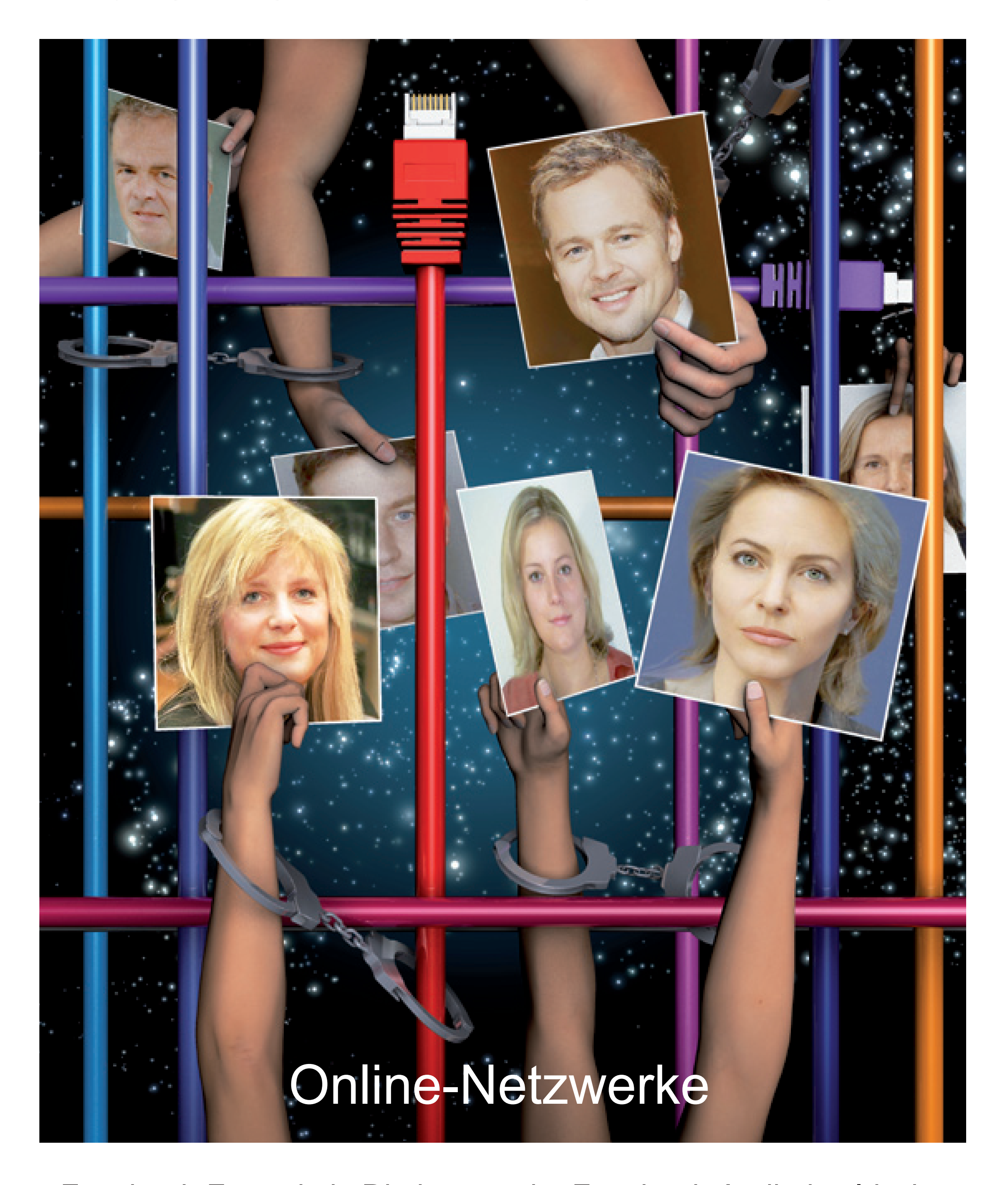
2/2012

Datenschutz Nachrichten

35. Jahrgang
ISSN 0137-7767
9,00 Euro



■ Facebook-Freunde in Dimitrovgrad ■ Facebook-Audit des Irischen Datenschutzbeauftragten ■ Social Swarm ■ Sozialdatenschutz bei inneradministrativen Prozessen ■ EGK – Too big to fail? Ein Zwischenbericht ■ Betriebliche Datenschutzbeauftragte ■ BigBrother-Awards 2012 ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechung ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Die in diesem Heft abgedruckten Artikel geben nicht durchgängig die Meinung der DANA-Redaktion wieder. Dennoch halten wir die Auseinandersetzung mit den vorgetragenen Argumenten für wichtig und sinnvoll.

Termine

Mittwoch, 1. August 2012
Redaktionsschluss DANA 3/12
Thema: Umfragen,
verantwortlich: Karsten Neumann, Sönke Hilbrans
Fragen und Anregungen bitte an:
neumann@baltic-privacy-management.eu,
shi@diefirma.net

Dienstag, 04 September 2012
Infoveranstaltung zum Beschäftigtendatenschutz
Brüssel. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Samstag, 27. Oktober 2012
DVD-Vorstandssitzung
Bonn. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Sonntag, 28. Oktober 2011
DVD-Mitgliederversammlung
Bonn.

Donnerstag, 1. November 2012
Redaktionsschluss DANA 4/12
Thema: Noch nicht bekannt

Freitag, 9. November 2012
FIfF Jahrestagung 2012
Hochschule Fulda
www.fiff.de

DANA

Datenschutz Nachrichten

ISSN 0137-7767

35. Jahrgang, Heft 2

Herausgeber

Deutsche Vereinigung für Datenschutz e.V. (DVD)

DVD-Geschäftstelle:

Rheingasse 8-10, 53113 Bonn

Tel. 0228-222498

Konto 1900 2187, BLZ 370 501 98, Sparkasse KölnBonn

E-Mail: dvd@datenschutzverein.de

www.datenschutzverein.de

Redaktion (ViSdP)

Karin Schuler

c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)

Rheingasse 8-10, 53113 Bonn

dvd@datenschutzverein.de

Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz

Frans Jozef Valenta, 53119 Bonn

valenta@t-online.de

Druck

Wienands Printmedien GmbH

Linzer Str. 140, 53604 Bad Honnef

wienandsprintmedien@t-online.de

Tel. 02224 989878-0

Fax 02224 989878-8

Bezugspreis

Einzelheft 9 Euro. Jahresabonnement 32 Euro (incl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe

Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen

Frans Jozef Valenta

Wen interessieren Nutzungsregeln?

Mal angenommen, Sie hätten beschlossen, Ihren Pfunden endlich den Kampf anzusagen, die neumodischen Fitnesscenter wären jedoch nichts für Sie. Da finden Sie eines Tages eine ansprechende Werbebroschüre eines ortsansässigen Sportvereins in Ihrem Briefkasten. Darin werden sehr detailliert einige neue und langjährige Mitglieder samt ihren Lebensumständen vorgestellt. Und fast alle sind mit dem Wunsch eingetreten, ihr Gewicht zu reduzieren und waren schließlich erfolgreich. Auch hören Sie in den nächsten Wochen von immer mehr Bekannten, dass auch sie Mitglied sind.

Und da das Trainieren im vertrauten Kreis sicherlich mehr Spaß macht als das einsame Laufen im Wald, schauen Sie eines Tages persönlich in der Geschäftsstelle des Vereins vorbei. Die nette Geschäftsführerin erläutert Ihnen, welche Vorzüge Sie als Mitglied zu erwarten haben. Besonders stellt sie heraus, dass Sie als Mitglied dieses Vereins in einer modernen Gemeinschaft trainieren, deren Mitglieder keineswegs nur aus Ihrer Heimatgemeinde stammen. Vielmehr unterhält der Verein beste Beziehungen zu Vereinen in aller Welt. Sie können bei Urlaubsreisen deren Sportstätten nutzen und von den Erfahrungen und Ratschlägen aller Mitglieder profitieren. Als die Dame hört, dass Sie in einem sehr gut beleumundeten Wohnviertel wohnen, scheint ihr Interesse nochmals zu steigen. „Und außerdem", lockt sie Sie weiter, „erheben wir keinen Mitgliedbeitrag". Unser Modell ist weltweit einmalig, denn wir haben finanzkräftige Sponsoren, die Ihnen ab und zu ein wenig Werbung überreichen.

Ihnen wird erläutert, dass Ihr Verein daher seinen Sitz nicht etwa, wie Sie dachten, in Ihrer Heimatgemeinde hat, sondern in Irland. Naja, macht nichts, denken Sie, was scheren mich die juristischen Spitzfindigkeiten, wenn ich doch nur Sport treiben will?

Fast unterschreiben Sie schon den Mitgliedsantrag, als Sie doch noch mal nach den Vereinsstatuten fragen, die Sie ja schließlich mitunterzeichnen. Die nette Dame druckst etwas herum, fängt aber schließlich unwillig an, den Text zu suchen. In einem verstaubten, unbeschrifteten Ordner wird sie schließlich fündig: 17 engbeschriebene Seiten, die den Mitgliedern die Einhaltung ganz bestimmter Verhaltensregeln auferlegen und dem Verein sehr weitgehende Rechte einräumen. Als Sie sich zum Lesen in eine Ecke zurückziehen, staunen Sie nicht schlecht:

Zur Nutzung der Sportstätten erhält jedes Mitglied eine Zutritts-Chipkarte, auf der jede sportliche Aktivität automatisch festgehalten wird. Wann Sie wo und wie lange, mit wem und mit welchem Erfolg trainiert haben, wie Ihre persönliche Leistungskurve aussieht, wie Sie im Vergleich mit anderen Mitgliedern abschneiden: all das wird minutiös erfasst. Zur Abrundung der Analyse beschäftigt der Verein außerdem einen eigenen Fotografen, der nicht nur die Sportstätten regelmäßig besucht. So entstehen Fotosequenzen von Trainingseinheiten, aber auch im privaten und beruflichen Umfeld der Mitglieder, wo der Fotograf regelmäßig auftaucht um Fotos zu schießen. Außerdem werden die Mitglieder regelmäßig zu Ihrer Einschätzung der anderen Mitglieder befragt. Diese Bewertungen fließen, wie alle anderen Angaben, in das Mitglieder-Profil ein und werden zur Erstellung eines so genannten Ernsthaftigkeits-Indexes verwendet, der das Mitglied in erster Linie motivieren soll.

Selbstverständlich ist das Training alleine nicht ausreichend, um Ihr Übergewicht in den Griff zu bekommen. Schließlich gehören auch gesunde Ernährung, genügend Schlaf, ausreichende Ruhepausen zu den richtigen Verhaltensweisen, die die persönliche Fitness bestimmen.

Also wird Ihr Sportverein Ihnen kostenlos und völlig unverbindlich den Kontakt zu Ernährungsberatern, Bioläden, Schlaflaboren, Matratzenproduzenten, Sportgeschäften und weiteren Dienstleistern herstellen. Genau gesagt: er wird Ihre vollständigen Daten zu Trainingsstand, Wohn- und Lebenssituation an diese weitergeben, damit eine möglichst spezialisierte Beratung stattfinden kann.

Da die Vielzahl möglicher Verwendungen kaum vorher einzugrenzen ist, gestatten die mit dem Mitgliedsantrag unterschriebenen Statuten dem Verein daher ganz pauschal, sämtliche zum Mitglied vorhandenen Daten nach eigenem Gutdünken kostenlos und weltweit zu nutzen.

Will man beispielsweise nicht, dass der Fotograf die ausführliche Fotoserie des eigenen Hauses (einschließlich der mit Bierflaschen gefüllten Mülltonne) an Ernährungsberater und andere weitergibt, so muss man rund ums Haus große Schilder „Fotos verboten" aufstellen. Vergisst man die Kennzeichnung (z. B. am rückwärtigen Eingang zur Garage), so soll das Verbot hierfür nicht gelten.

Ab und zu schickt der Verein auch einen der Trainer vorbei, der nicht immer klingelt, sondern manchmal auch nur durch die Fenster schaut. Dies findet insbesondere dann statt, wenn der Verein weiß, dass sich mehrere Vereinsmitglieder bei einem Sportkameraden verabredet haben. Es wird dann notiert, wer mit wem gegessen, gefeiert, oder Schach gespielt hat. Sobald man als Gastgeber den Fotografen oder den Trainer bemerkt, muss man die Gäste darauf hinweisen und sofort klären, ob sie damit einverstanden sind, in Besuchsberichten und Fotos des Gastgebers zu erscheinen.

Finden derartige Treffen während einer eigentlich vereinbarten Trainingseinheit statt, so wird der Ernsthaftigkeitsindex sofort herabgestuft. Der Verein wird Ihnen dann auch vorschlagen, sich in Zukunft eher mit bestimmten anderen Mitgliedern zu treffen, die Ihrem Trainingsplan zuträglicher erscheinen.

Schließlich finden Sie sehr versteckt auch noch eine Bestimmung über die Höhe des Mitgliedsbeitrags: Sie lautet lapidar: Wir garantieren nicht, dass die Mitgliedschaft immer kostenlos bleiben wird, aber wenn Sie uns frankierte und mit Ihrer Adresse versehen Briefumschläge in ausreichender Zahl bereitstellen, informieren wir Sie, bevor wir Ihr Konto bei einer evtl. Änderung belasten.

Würden Sie Mitglied in einem solchen Verein werden? Oder sind Sie es schon? Und wollen es bleiben? Dann sollten Sie sich zumindest einen Eindruck darüber verschaffen, welche Leistungskurven, Beurteilungen Ernsthaftigkeitsindizes und sonstige Daten sich im Laufe der Zeit angesammelt haben. Ein Blick auf www.europe-v-facebook.org hilft beim organisierten Vorgehen.

Und wenn Sie sich durch diesen Text in der Facebook-üblichen Schriftgröße gekämpft haben, dann werden Sie die nächsten Seiten dieses Heftes hoffentlich ganz besonders genießen, wünscht Ihnen Karin Schuler.

Autorinnen und Autoren dieser Ausgabe:

Helmut Eiermann

Leiter des Bereichs Technik beim Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, eiermann@email.de

Der Artikel gibt die persönliche Auffassung des Autors wieder.

Prof. Dr. Thomas Hoeren

Leiter des Instituts für Informations-, Telekommunikations- und Medienrecht der Westfälischen Wilhelms-Universität Münster, hoeren@uni-muenster.de

Jan Kuhlmann

Rechtsanwalt und IT-Berater in Karlsruhe, Jan_Kuhlmann@yahoo.de

Karsten Neumann

Vorstandsmitglied der DVD, Landesbeauftragter für Datenschutz Mecklenburg-Vorpommern a.D., Associate Partner der 2B Advice GmbH, neumann@baltic-privacy-management.eu.

Katharina Nocun, Leena Simon, padeluun und Freunde

Mitarbeiter des FoeBuD e.V., Bielefeld, socialswarm@foebud.org

Dr. jur. Georgios Samartzis

Mag.rer.publ., Jurist und Bereichsleiter in der Agentur für Arbeit Darmstadt und trägt in dieser Funktion Mitverantwortung für die Einhaltung des Sozialdatenschutzes in der Arbeitsagentur, samartzis@gmx.de

Thomas Hoeren

My friends from Dimitrovgrad. Ein Selbstversuch

Nachdruck eines Online-Artikels für den Deutschlandfunk[1] vom 9.2.2012 –
mit freundlicher Genehmigung von Autor und Redaktion

Wer kennt Sybille Epping? Thomas Hoeren, Professor am Institut für Informations-, Telekommunikations- und Medienrecht der Westfälischen Wilhelms-Universität Münster führt im Selbstversuch vor, wie unecht die virtuelle Welt der Freundschaftsnetzwerke sein kann, und dass echte Netzwerk-Junkies selbst von deutlichen Hinweisen auf Fälschungen gar nichts wissen wollen…

Seit einigen Wochen macht eine junge Deutsche die kleine bulgarische Stadt Dimitrovgrad virtuell unsicher. Binnen weniger Tage hat sie viele hundert Freunde bei Facebook gefunden, vor allem in den weiterführenden Schulen in Dimitrovgrad. Aus den privaten Fotoalben ihrer „Freunde" kopierte sie die schönsten Fotos und stellte sie wieder im öffentlichen Bereich ihrer eigenen Facebook Website der Allgemeinheit zur Verfügung. Einige Fotos übernahm sie sogar als die eigenen, insbesondere Geburtsfotos und Einschulungsportraits. Die „Freunde" meldeten sich nie; einige von ihnen ergänzten die gestohlenen Fotos sogar noch mit Hinweisen auf ihre eigenen Namen. Und so hätte das Ganze über Monate weitergehen können – hätte sich nicht die Dame kürzlich geoutet. Denn die Wohlproportionierte im kleinen Schwarzen bin ich. Das genannte Dimitrovgrad-Experiment sollte dazu dienen, herauszufinden, wie sich die junge Generation in einer fernen Kleinstadt in Facebook darstellt und wie sie mit ihren Freunden und ihrem virtuellen Privatwelten umgehen. Der Befund ist erschreckend.

Die Sensibilität für den Wert von Privatheit scheint verloren gegangen zu sein. Fotos bei Facebook sind fungible Informationsgüter, genauso wie die Eigenschaft, „Freund" zu sein. Viele der bulgarischen Jugendlichen hatten deutlich mehr als 2.000 „Freunde", offensichtlich eine wirre Ansammlung von mehr oder weniger flüchtigen Kontakten. Viele stellten selbst intimste Fotos für die Öffentlichkeit ins Netz, einschließlich der fast obligatorischen Saufpartys, muskelprotzender Fitnessbesucher oder leicht bekleideter Strand-Eskapaden. Der Befund deckt sich mit vielen Beobachtungen auch in anderen Web 2.0-Anwendungen. Er wird meist zum Anlass genommen, zwischen zwei verschiedenen Lagern in der Diskussion rund um Facebook zu unterscheiden. Die einen verteufeln Facebook und kritisierten wie der Adler in der Muppet-Show den Sittenverfall im Web. Die Gegenseite beruft sich auf US-amerikanische Ideen der Post-Privacy. Danach soll die hohe Sensibilität für Datenschutz und Persönlichkeitsrechte ein historisches Fossil sein, das im Zeitalter des Internets seine Bedeutung verloren habe.

Meines Erachtens sollte abseits dieser Extrempositionen erst einmal der Befund tiefer analysiert und dann differenzierend bewertet werden. Privat und öffentlich waren immer schon Begriffe, die inhaltlich starken Veränderungen unterworfen waren. Aristoteles sah die Abgrenzung zwischen öffentlich und privat als eine von Staat (Polis) und Haus (Oikos). Diese Kategorien wurden dann im Laufe des 18. Jahrhunderts mit der Etablierung des Bürgertums im Sinne einer herrschaftsemanzipierten Sphäre eines umfassenden Diskurses umdefiniert. Die Öffentlichkeit als emanzipatorischer Ort einer bürgerlichen Gesellschaft unterliegt seitdem einem enormen Strukturwandel, verfällt zugunsten einer Tyrannei der Intimität. An die Stelle des „Es", des „Wir", der Gemeinschaft, des Sozialengagements, tritt das selbstreferentielle „Ich". Entscheidend ist es, sich selbst auszudrücken, die Selbstinszenierung, private Geschwätzigkeit. Vor mir zieht auf der Facebook-Pinnwand ein Strom der Belanglosigkeiten vorbei. Vereinsamte Dulchanas und Dugonevs, in ihren kärglichen Zimmern hockend, an einem stalinistisch errichteten Nicht-Ort mit Plattenbauten. Männer stehen vor dem Spiegel in Bodybuilding-Pose, mit BMW oder aufgemotztem Moped, bei Sauf-Partys und mit aufgebretzelter „Tusse", mit Detailfotos ihrer Tattoos. Kleine Mädchen werfen sich in schlechte Schale, in Knutschpose, umgeben von den „harten Jungs" oder ihrem Lieblingsstofftier. Eine Timeline des Datenmülls zieht sich durch die Freundesliste und gibt den „friends" das Gefühl, dabei zu sein und nichts verpasst zu haben.

Dem Siegeszug der Intimität steht paradoxerweise ein Siegeszug des Öffentlichen gegenüber. Denn das Private wird in Zeiten von Google+ nicht mehr als privat wahrgenommen, sondern als öffentliches Gut, als jederzeit transferierbarer Datensatz. Dementsprechend verstehen die Jugendlichen auch nicht, was das Problem von Facebook sein soll. Es ist ihnen egal, dass sie sich mit der Bereitstellung ihrer Fotos und Texte selbst kommerzialisieren und sich selbst in die Hände eines Unternehmens begeben, dessen Datenschutzkonzept mehr als nebulös ist und das wie selbstverständlich alle Persönlichkeitsprofile für eigene kommerzielle Zwecke nutzt. Aus dem „Right to be let alone" ist ein „Right to perform alone" geworden, ein Recht auf Selbstinszenierung. Es entsteht ein neues Spiel virtueller sozialer Kontexte, mit immer neuen Ad-hoc-Wirklichkeiten. Selbst die traditionellen Zugangssperren zu Gunsten von Kindern und Jugendlichen versagen. In Dimitrovgrad fand ich schon Zehn- und Elfjährige, die wie Erwachsene auf ihren Seiten posieren. Wie Marshall McLuhan prophezeite, stülpen sich die Kids um „wie Amphibien", den „Panzer nach

Innen", die seelischen „Weichteile nach Außen".

Dieser Wandel bringt vielfältige Änderungen auch für die Rechtsordnung mit sich. Das Recht am eigenen Bild wird z.B. traditionell als Abwehrrecht gegen eine Verwendung des Bildes ohne Zustimmung des Abgebildeten gesehen. Wie Ladeur schon zu Recht vor Jahren festgestellt hat (NJW 2004, 393 ff.), entspricht diese Konstruktion nicht mehr den Bedürfnissen der Postmoderne. In Web 2.0-Zeiten veröffentlichen sich die Inhaber der Persönlichkeitsrechte selbst massiv, wollen dann aber auch die Grenzen der Verbreitung solcher Informationen selber bestimmen. Ladeur schlägt daher vor, ein Recht auf Verfügung über die eigene Selbstdarstellung in der Öffentlichkeit zu kreieren. Aus dem Right of Privacy würde so ein Right of Publicity. Meines Erachtens wird aber auch das nicht hinreichend dem Wesen des Web 2.0 gerecht. Ein Recht auf Selbstinszenierung ist als prozedurales Recht aufzufassen. Facebook und Co. werden von den Kindern Dimitrovgrads als eine Art Spiel betrachtet, mit eigenen Spielregeln. Im Vertrauen auf diese Spielregeln tauchen die Jugendlichen in die Facebook-Welt ab. Die Spielregeln sind zum Teil nicht rechtlicher Natur; hier geht es darum, sich nach Maßgabe noch weitgehend unerforschter Sozialregeln mit allen möglichen Insider-Tricks möglichst viele Freunde und möglichst hohe Internet-Reputation zu besorgen. Die Spielregeln umfassen aber auch normative Regeln. Oberstes Gebot muss hier vor allem die Transparenz haben. Wer sich auf Facebook einlässt, muss klar verstehen können, nach welchen Regeln man hier was wie vornehmen oder stoppen kann. Davon ist Facebook meilenweit entfernt, da das Unternehmen wie ein Moving Target auftritt. Es ändert sehr häufig die Regeln, zuletzt bei der Einführung der Timeline. Wird das Unternehmen dann kritisiert, werden die Regeln wieder blitzschnell geändert. Die Regeln selbst sind unglaublich kompliziert und stellen gerade nicht auf die Zustimmung ab, sondern auf ein sehr komplexes Widerspruchssystem. Das Spiel mit der Selbstinszenierung ist im Übrigen ein sehr dynamisches, gerade auch aus der Sicht der Spieler. Es muss gewährleistet sein, dass die Spieler ihre eigene Selbstinszenierung wieder ihrem sich verändernden Alters- und Lebenszustand anpassen. Insofern ist in der Tat die Möglichkeit einer schnellen und grundlegenden Löschung von Daten von zentraler Bedeutung, ein umfassendes Recht auf Vergessen – gerade auch gegenüber Facebook selbst. Es verstößt im übrigen auch gegen das Recht auf Selbstinszenierung, wenn jemand liebevoll auf unterschiedlichen Plattformen neue Identitäten erfindet und differenzierte Wahlen bezüglich der Datenfreigabe vornimmt – und dann Unternehmen oder der Staat seinerseits anfängt, die entsprechenden Daten zu bündeln. Der Nutzer verliert auf diese Weise die Verfügungsgewalt über die Informationen. Ein solcher Akt kann auch nicht dadurch legitimiert werden, dass dies ja wohl im wohlverstandenen Interesse des Nutzers sei. Die Rechtsordnung stellt nicht auf wohlverstandene Interessen ab, sondern darauf, dass jemand selbst von sich aus eine bestimmte Inszenierung gewählt hat. Insofern ist gerade das von Google jüngst angekündigte Zusammenführen der einzelnen Nutzerdienste ein fundamentaler Angriff auf die Privatsphäre. Schließlich wird auch die alte Differenzierung von Meinungen und Tatsachenbehauptungen aus dem traditionellen Presserecht der neuen Lebenswirklichkeit in den Medien nicht gerecht. In Facebook geht es nicht darum, nur wahre Tatsachen zu verbreiten. Die Abgrenzung von Meinungen und Tatsachen ist ohnehin schon schwierig; sie verläuft aber bei den sogenannten Sozialen Medien ins Leere. Da dient die Selbstinszenierung gerade dazu, sich groß zu machen, sich aufzuplustern, gegebenenfalls auch pseudonym aufzutreten. Entscheidend ist es, die Aufmerksamkeit für sich und seine Person zu erhöhen. Ich selbst mache da aber nicht mehr lange mit. Ich werde mein kleines Dimitrovgrad-Experiment jedenfalls bald beenden. Die Schulen und Lokalzeitungen in Bulgarien habe ich schon informiert, bislang ohne Reaktion. Nun gut – dann kommt bald das Ende für meine vielen „friends from Dimitrovgrad".

1 http://diskurs.dradio.de/2012/02/09/my-friends-from-dimitrovgrad-rechtliche-uberlegungen-zur-veranderung-von-privatem-und-offentlichem-raum-in-zeiten-der-digitalisierung/

Helmut Eiermann

„Best Practice" – Approach oder Appeasement.

Zum Facebook-Audit des Irischen Datenschutzbeauftragten

Ende 2011 untersuchte der Irische Datenschutzbeauftragte im Rahmen eines Audits die Datenverarbeitung durch Facebook für die europäischen Nutzer des Sozialen Netzwerks. Die Prüfung erfolgte durch den Data Protection Commissioner Ireland (DPC), da Facebook mit der Facebook Ireland Ltd. eine europäische Niederlassung unterhält. Der Bericht wurde am 21.12.2011 veröffentlicht; er umfasst den eigentlichen Auditbericht sowie fünf Anhänge.[1]

Den Hintergrund des Audits bildete ein vielfarbiges Mosaik aus offenen Fragen zu Art und Umfang der Verarbeitung personenbezogener Daten durch Facebook[2], einer Reihe von Anzeigen bei der Irischen Datenschutzaufsichtsbehörde[3], ungeklärten Rechtsfragen und unterschiedlichen Positionen hinsichtlich des anwendbaren Rechts und damit

verbundener Zuständigkeiten. Selbst in den Gutachten der wissenschaftlichen Dienste zweier Parlamente, des Bundestages[4] und des schleswig-holsteinischen Landtags,[5] blieb aufgrund der komplexen und unübersichtlichen Rechtslage eine abschließende datenschutzrechtliche Bewertung offen. In der Tat führt die Konstellation, bei der ein global agierendes US-amerikanisches Unternehmen seine innovativen und komplexen Dienste auf unterschiedlichen Märkten anbietet, deren rechtliche Rahmenbedingungen darauf nicht oder nur zum Teil ausgerichtet sind, zu Fragen, für die eine Antwort zu finden nicht einfach ist. Umso wichtiger scheint es, herauszuarbeiten, wo bei der Datenverarbeitung jedenfalls Zweifel an der Vereinbarkeit mit der jeweiligen Rechtsordnung bestehen.

Methodisch fußte das Audit, worauf der Irische Datenschutzbeauftrage ausdrücklich hinweist, auf einem Prüfkonzept[6] für sogenannte "compliance audits", d.h. Untersuchungen, inwieweit die Verfahrensweisen, Leitlinien, Systeme und Datenspeicherungen datenschutzrechtlichen Anforderungen entsprechen ("to assess wether the organisation is generally in compliance with requirements under data protection legislation"; Fußnote 6, Seite 4). In technischer Hinsicht wurde der DPC von der Universität Dublin unterstützt.

Die im Prüfbericht dargestellten Ergebnisse haben ein unterschiedliches Presseecho hervorgerufen. Während Der Spiegel von einem "recht positiven Prüfbericht" sprach[7] oder Die Zeit davon, dass der Irische Datenschützer Facebook "entlastet"[8], waren Die Welt[9] und die Frankfurter Rundschau[10] der Auffassung, dass Facebook beim Datenschutz nachbessern müsse. Die Süddeutsche Zeitung wiederum sah den Irischen Datenschutzbeauftragten erfolgreich darin, Facebook zu Zugeständnissen gezwungen zu haben.[11] Facebook selbst sieht den Auditbericht als Beleg dafür, dass seine Angebote mit irischem und europäischem Recht in Einklang stehen.

In der Tat liefert der Prüfbericht Argumente für beide Sichtweisen. Es kann daher erhellend sein, die von ihm dargestellten Ergebnisse und daraus folgende Empfehlungen im Licht des zugrunde liegenden Auditkonzepts und dessen Anspruch, eine Compliance-Prüfung darzustellen, zu bewerten. Nachfolgend sind daher wesentliche inhaltliche Punkte dargestellt, bei denen der Irische Datenschutzbeauftragte Defizite oder Verbesserungsmöglichkeiten angesprochen hat. Zum Teil hat Facebook auf die Feststellungen bereits mit geänderten Verarbeitungsrichtlinien reagiert oder eine Prüfung der Empfehlungen in Aussicht gestellt. Gleichwohl handelte es sich zunächst um bestehende Mängel:

- Zwingend notwendige Verbesserungen bei den Privatsphären-Einstellungen (Auditbericht (Fußnote 1), Seiten 36, 39, 42). Der Irische DSB mahnt an, dass bei den Privatsphären-einstellungen Verbesserungen erfolgen müssen. Außerdem müssen die Nutzer besser als bislang dazu befähigt werden, informiert in die einzelnen Verarbeitungen ihrer Daten durch Facebook einzuwilligen („Facebook must work towards simpler explanations…easier accessibility…informed choices").
- Speicherung von Daten über die Kenntnisnahme von Werbeanzeigen (a.a.O. Seiten 56/61). Facebook speichert Daten darüber, welche Anzeigen ein Nutzer angeklickt hat, bislang unbegrenzt. Dies wurde seitens des Irischen DSB als inakzeptabel angesehen („unacceptable"). Künftig wird die Speicherung dieser Daten auf 24 Monate begrenzt.
- Fehlende Möglichkeiten für die Nutzer, Posts, Messages, Freundschaftsanfragen etc. zu löschen (a.a.O., Seiten 70/77). Der Irische DSB mahnt hier notwendige Löschfunktionen an („ability should be provided"). Darüber hinaus sollten die Nutzer besser darüber informiert werden, wie mit gelöschten oder zurückgenommenen Inhalten verfahren wird („should be improved").
- Datenspeicherung auch nach Wegfall des Verarbeitungszwecks (a.a.O., Seiten 74, 75, 78).
- Unzureichende Information der Nutzer über die Verarbeitung von Nutzungsdaten (a.a.O., Seiten 74, 79).
- Fehlende Regelungen zur Löschung inaktiver oder deaktivierter Benutzerkonten (a.a.O., Seiten 75, 79).
- Unangemessene („not appropriate") und besorgniserregende („obvious concern") Speicherung der über Social-Plugins erhobenen Daten (a.a.O., Seiten 83, 85).
- Unzureichende Unterrichtung der Nutzer und fehlende Steuerungsmöglichkeiten bezüglich der Weitergabe von Daten an Drittanwendungen (a.a.O., Seiten 89, 93, 94, 96). Der Irische Datenschutzbeauftragte beklagt die bestehende Komplexität der Mechanismen beim Datenzugriff durch Drittanwendungen und mahnt Verbesserungen bei der Information der Nutzer und der Möglichkeiten, einen solchen Datenzugriff zu steuern an („Users must be empowered via appropriate information and tools to make a fully informed decision when granting access to their information to third party applications").
- Fehlende Dokumentation von Datenverarbeitungen und Verfahrensweisen („not formally documented") bzw. fehlendes formales Sicherheitskonzept (a.a.O., Seiten 108,110).
- Besorgniserregender Umfang („concerned") der Zugriffsmöglichkeiten von Facebook-Mitarbeitern auf Nutzerdaten (a.a.O., Seiten 108, 110)
- Keine zeitnahe Löschung der Daten von gelöschten Benutzerkonten (a.a.O., Seiten 116, 117). Der Irische DSB bemängelt hier, dass es nach der gegenwärtigen Verfahrensweise bis zu 90 Tage dauern kann, bis eine Löschung erfolgt. Section 6 des irischen Datenschutzgesetzes (Data Protection Act 1988) sieht eine maximale Frist von 40 Tagen vor.
- Verbesserungsbedürftige Funktionen zur Steuerung, welche Personen(kreise) Kenntnis von Nutzerpostings erhalten können („recommend … increased functionality"; a.a.O., Seite 130).
- Überarbeitungsbedürftige Datenschutzbestimmungen im Zusammenhang mit der Nutzung von Facebook-Credits („recommend … significantly expanded"; a.a.O. Seite 133).
- Kenntnisdefizite bei den Mitarbeitern von Facebook („compliance requirements ... not fully understood") bezüglich der rechtlichen Anforderungen beim Direktmarketing (a.a.O., Seiten 145, 148).

- Notwendigkeit zusätzlicher Maßnahmen, um bei der Einführung neuer Facebook-Funktionen die Konformität mit irischem und europäischem Datenschutzrecht zu gewährleisten (a.a.O., Seite 148). Dazu zähle auch, dass Facebook die Entwickler und Betreiber von Drittanwendungen auf die Einhaltung des europäischen Datenschutzstandards verpflichten müsse („a remaining legitimate concern … requires additional measures“)

Trotz dieser Punkte sah der Irische Datenschutzbeauftragte bei der Datenverarbeitung durch Facebook Ireland Ltd. offenkundig keine Kollission mit bestehenden Datenschutzvorschriften ("The recommendations in the Report do not carry an implication that Facebook Ireland's current practices are not in compliance with Irish Data Protection law; a.a.O. Seite 4). Dieser Hinweis in der Executive Summary muss wohl dahingehend verstanden werden, dass das Audit den ersten Schritt der Prüfung darstellte, bei dem im Sinne eines "Best Practice Approach" die Anforderungen einer "fairen" Datenerhebung und -verarbeitung untersucht wurden, und erst in einem zweiten Schritt Mitte 2012, nach Umsetzung einer Reihe von Empfehlungen, eine abschließende Bewertung erfolgen soll.

Es mag auch damit zu tun haben, dass Facebook bereits während des Audits Maßnahmen in die Wege geleitet oder angekündigt hat, um den Datenschutz zu verbessern und eine Fortführung des Audits für 2012 vereinbart wurde. In Rechnung gestellt wurde auch, dass das immense Wachstum von Facebook innerhalb kürzester Zeit dazu geführt habe, dass die Struktur des Unternehmens und seine Geschäftsprozesse mitunter damit nicht hätten Schritt halten können. Der Auditbericht scheint erkennbar davon geprägt, die Bemühungen Facebooks um eine Verbesserung des Datenschutzes in bestimmten Bereichen anzuerkennen.

Die beschriebenen Mängel sowie die Einlassungen Facebooks im Bericht belegen jedoch, dass Facebook häufig hinter anerkannten Datenschutzstandards zurückbleibt, z.B. bei essentiellen Fragen wie der Transparenz der Datenverarbeitung und der informierten Einwilligung der Nutzer.

Was bleibt? Zumindest die Aussage eines Landesdatenschutzbeauftragten, dass obwohl die Anforderungen an die Trinkwasserqualität europaweit einheitlich vorgegeben seien, man in manchen Regionen dennoch lieber zu abgefülltem Mineralwasser greife.

1 http://www.dataprotection.ie/docs/21/12/11_-_Report_of_Data_Protection_Audit_of_Facebook_Irela/1182.htm

2 https://forbrukerportalen.no/filearchive/ncc_complaint_facebook_zynga_1_.pdf

3 http://europe-v-facebook.org/DE/Anzeigen/anzeigen.html

4 http://www.sebastian-blumenthal.de/files/sblumenthal/uploads/documents/gutachten_facebook_final.pdf

5 http://www.landtag.ltsh.de/infothek/wahl17/umdrucke/2900/umdruck-17-2988.pdf

6 http://www.dataprotection.ie/documents/enforcement/AuditResource.pdf

7 http://www.spiegel.de/netzwelt/netzpolitik/soziales-netzwerk-irischer-datenschuetzer-verteidigt-facebooks-klarnamenzwang-a-805121.html

8 http://www.zeit.de/digital/datenschutz/2011-12/irischer-datenschuetzer-facebook-bericht/komplettansicht

9 http://www.welt.de/wirtschaft/webwelt/article13779212/Facebook-muss-fuer-Irland-Datenschutz-verbessern.html?config=print

10 http://www.fr-online.de/digital/datenschutz-in-sozialen-netzwerken-facebook-muss-beim-datenschutz-nachbessern,1472406,11341474.html

11 http://www.sueddeutsche.de/digital/pruefbericht-zur-privatsphaere-irlands-datenschuetzer-zwingt-facebook-zu-zugestaendnissen-1.1241513

Katharina Nocun, Leena Simon, padeluun und Freunde

We are the Social Network, We are the Social Swarm

Soziale Netzwerke, speziell Facebook, sind spannend und erfolgreich. Doch alle Macht ist in der Hand eines Konzerns. Das muss sich ändern, sagen die Begründerinnen des Projekts „Social Swarm" und laden ein, mit zu machen. In Arbeit ist eine weltweite Kampagne, die einlädt, Softwaremöglichkeiten zu evaluieren, Grafik und Oberflächen zu entwickeln und wenn es dann soweit ist, zig Millionen Menschen zum Wechsel auf die gute Seite der Macht zu überzeugen. Sicher keine kleine Aufgabe.

Soziale Netzwerke sind für immer mehr Menschen ein fester Bestandteil ihres Lebens. Dabei beschränkt sich die Nutzung von *Social Networks* längst nicht mehr auf das Privatleben sondern hat auch Einzug in die politische und soziale Öffentlichkeit gehalten. Es scheint, als wäre die antike Agora auferstanden. Denn auf dem virtuellen Marktplatz der sozialen Netzwerke werden auch Widerstand organisiert und eine kritische Masse mobilisiert. Es scheint, als haben soziale Netzwerke das Potential, Teil einer neuen Infrastruktur für Demokratie im digitalen Zeitalter zu werden.

Doch der Vergleich zu der Agora im antiken Griechenland hinkt. Während das Internet von einer dezentralen Struktur getragen wird, gibt es unter den sozialen Netzwerken einen klaren Marktführer. Und der öffentliche Raum, der innerhalb dieser Netzwerke geschaffen wird, unterliegt den Allgemeinen Geschäftsbedingungen eines global agierenden Konzerns. Wer *Social Media* für sich nutzen möchte, kommt kaum noch an Facebook vorbei. Datenschützer und Bürgerrechtlerinnen betrachten diese Entwicklung mit großer Sorge. Der virtuelle Raum bei Facebook ist keineswegs öffentlich in dem Sinne, dass alle frei ein- und austreten können. Der Eintritt ist nur scheinbar kostenlos, aber nicht kostenfrei.

Die Datenkrake Facebook streckt mit dem Like-Button und Facebook Analytics seine Tentakel nach immer größeren Bereichen des Nutzungsraumes im Internet aus. Das Geschäft mit personalisierter Werbung brummt. Daher werden die Rechte der Nutzer stetig an den wachsenden Datenhunger angepasst. Facebooks Kapital sind die Daten von Teilnehmerinnen und Teilnehmern. Und das sind nicht (nur) Name und Anschrift und ein paar Bilder, sondern aggregierte Daten, Beziehungsgeflechte, Kontaktinformationen, Verhalten und mehr. „Hier wächst eine ‚Gated Community' globalen Ausmaßes heran, eine abgeschlossene Gesellschaft, in der ein Konzern die Regeln macht", beklagte Rena Tangens anlässlich der Verleihung des Big Brother Awards 2011. In ihrer Laudatio[1] beschreibt sie Facebook als „eine Datenkrake mit unendlichem Appetit – und die Leute begeben sich freiwillig in ihre Fangarme und füttern sie." Mit der Bereitstellung immer neuer Dienste und der Integration immer weiterer Kommunikations- und Interaktionskanäle drängt sich Facebook als unentbehrliche Plattform seinen Nutzern auf und ist auf dem besten Wege, ein nie gesehenes Datenmonopol zu schaffen.

Viele Menschen, die unzufrieden mit dieser Unternehmenspolitik sind, sehen sich in einem Dilemma – entweder auf die Vorzüge des digitalen gemeinsamen Raumes durch Nichtteilnahme verzichten oder Privatsphäre und Persönlichkeitsrechte beim Login an der Tür zur *Gated Community* abgeben. Folglich scheint es nur eine Möglichkeit zu geben: Entweder auf den Kontakt zu den vielen Menschen verzichten, die nur noch über Facebook erreichbar sind, oder selbst mitverantwortlich zu sein, dass mehr und mehr Menschen zu Facebook kommen.

Mit der Nutzung des Netzwerks steigt die kritische Teilnehmendenmasse des Monopolisten Facebook weiter an. Und weil „alle" dabei sind, kommen auch die anderen hinzu. Der Teufel scheißt halt immer auf den größten Haufen, weiß der Volksmund so derb wie treffend zu sagen. Mit zunehmender Abhängigkeit der Menschen von einer einzigen Plattform nimmt die Marktmacht des Unternehmens zu. In dem Wissen, keiner Konkurrenz durch Plattformen mit ähnlich großem Nutzerinnenkreis ausgesetzt zu sein, kann Facebook den Nutzern Bedingungen diktieren, die nicht in deren Interesse sind. Interessen von Strafverfolgungsbehörden und der Werbeindustrie werden dabei über die Persönlichkeitsrechte der Nutzerinnen gestellt.

In einer Demokratie gehört öffentlicher Raum zur kritischen Infrastruktur der freien Gesellschaft, da dort zentrale Prozesse der öffentlichen Debatte stattfinden. Das größte Kapital jedes sozialen Netzwerkes sind seine Teilnehmerinnen und Teilnehmer. Ohne eine kritische Nutzerinnenmasse ist ein Netzwerk wertlos. Für eine freie Gesellschaft bedeuten Datenmonopolisten wie Facebook jedoch den Ausverkauf des digitalen öffentlichen Raumes und die Abkehr vom dezentralen Paradigma der Netze. Tim Berners-Lee[2] selbst beklagte, dass Facebook das Internet ausblute: Viele Nutzer halten sich nur noch in Facebook auf. Es gibt bereits Telefonprovider, die zwar keinen Internet-Browser, aber einen Facebookzugang zum Smartphone ‚beilegen'.

Der Mensch ist ein soziales Wesen. Dies wird sich auch im digitalen Zeitalter nicht ändern. Es liegt an den Nutzerinnen, sich den Raum, den sie

für die Entfaltung ihrer Persönlichkeit brauchen, auch digital zu erstreiten. In der Vergangenheit kam es immer wieder zu Protesten der Nutzer gegen die Unternehmenspolitik von Facebook. Den Menschen ist der Umgang des Unternehmens mit Daten nicht geheuer, so viel ist sicher. Die Menschen wünschen sich ein echtes soziales Netzwerk, sie wünschen sich eine Alternative – ein soziales Netzwerk, das den Namen „sozial" auch verdient: einen sozialen Schwarm, neudeutsch: „Social Swarm".

Social Swarm – Quo vadis?



Soziale Netzwerke sind ein Phänomen das weit über Facebook hinausgeht und das es auch ohne Internet schon gab. Mittlerweile existieren zahlreiche Alternativen zu Facebook. Allein die immensen Spenden, die das Projekt Diaspora auf sich vereinigen konnte, zeigt, wie ernst es den Nutzern um ihren digitalen öffentlichen Raum ist. Dabei ist vor allem wichtig, dass Menschen nicht ausgesperrt werden können und weiterhin Wahlfreiheit über die Plattform haben, die sie nutzen möchten.

Wie groß der Wunsch nach Alternativen zu Facebook ist, zeigt sich nicht zuletzt auch dadurch, dass es mittlerweile viele Dutzend Softwareprojekte gibt, die sich zum Ziel gesetzt haben, die Marktmacht Facebooks zu brechen. Doch genau in der Verstreutheit liegt das Problem. Um Facebook von der Monopolposition zu vertreiben, muss eine kritische Nutzerinnenmasse geschaffen werden. Erst wenn ein Angebot von genug Menschen für gut befunden wurde, kann eine echte Agora geschaffen werden, ein Raum für Menschen und Meinungen, der nicht Privateigentum eines Unternehmens ist, ein Freiraum für Demokratie und Menschenrechte.

Was wir haben

Was wir wollen

Benutzer

Daten

Firma

Nur wenn die Alternativprojekte zusammenarbeiten, wird es möglich sein, gemeinsam eine genügend kritische Masse zu versammeln. Doch Kooperation ist nicht immer einfach und es braucht einen neutralen Ort, an dem die Protagonisten aufeinander zugehen können. Social Swarm ist kein weiteres Softwareprojekt, sondern die Moderation eines Prozesses, der lange schon überfällig ist.

Dezentrale Netzwerke bieten eine echte Alternative. Machtkonzentration in den Händen weniger müssten nicht länger in Kauf genommen werden. Die Teilnehmerinnen selbst werden zu Anbieterinnen des Netzwerkes und bekommen so die Kontrolle über ihre Daten zurück. Ein dezentraler Ansatz bedeutet dabei eine Rückbesinnung auf die Grundgedanken des World Wide Web.

Offene Schnittstellen und die Nutzung freier Software sind weitere Eigenschaften, die Sicherheit gewährleisten und Schutz vor neuen Monopolen bieten können. Erst eine dezentrale, freie und offene Plattform schafft Raum für ein echtes „soziales" Netzwerk, das seinen Namen auch verdient hat. Einfache Bedienung sowie eine gute grafische Nutzeroberfläche sind weitere Anforderungen, die für das Zustandekommen eines Social Swarms gegeben sein müssen.

Nur ein öffentlicher Raum, der aus der Vielheit seiner Teile hervorgeht, kann Raum geben für öffentliche Debatten und die Entfaltung der eigenen Persönlichkeit, frei von Macht, Kontrolle und Zensur. Die daraus entstehenden Synergien könnten zu einer echten Bereicherung für Nutzer und Zivilgesellschaft führen. Eine freie Gesellschaft darf nicht auf das Angebot eines kommerziellen und zudem monopolistischen Anbieters digitaler Öffentlichkeit angewiesen sein. Die Funktion sozialer Plattformen in der digitalen Gesellschaft von morgen ist zu wichtig, um sie in die Hände eines einzelnen Konzerns zu legen.

Join the Social Swarm

Ziel der Kampagne ist es, einen Social Swarm zu erzeugen, der im Rahmen eines Aktionstages Facebook den Rücken kehren wird. Es gibt viele Teilnehmerinnen, die unzufrieden sind. Flankiert werden sie von amtlichen und freien Datenschützern. Unübersichtliche Privatsphäreneinstellungen, undurchsichtige Unternehmenspolitik und gigantische Datenspeicher sind gute Gründe, um nach einem besseren, einem „sozialen" Netzwerk zu suchen.

Der Social Swarm hat sich mit diesem Ziel zusammengefunden und arbeitet an der Umsetzung dieser Vision. Der Weg ist dabei zugleich auch das Ziel und während des gemeinsamen Entscheidungsfindungsprozesses wächst der Schwarm stetig weiter. Die Debatte um die am besten geeignete Software, erfolgversprechende Strategien für Wechselaktionen und die Suche nach Bündnispartnern ist bereits angelaufen. Es ist ein ergebnisoffener Prozess, bei dem sich jeder einbringen kann. Der Social Swarm ist so bereits jetzt ein soziales Netz, derzeit noch heimatlos, über Mailinglisten und Wikis verstreut, auf der Suche nach einem neuen Ort, an dem man sich niederlassen möchte, einem Ort ohne Einlasskontrollen und

Mauern. Ein Zuhause, in das man seine Freunde gerne und guten Gewissens einladen möchte.

Damit die Aktion ein Erfolg wird, brauchen wir jede und jeden Einzelnen. Denn der Social Swarm lebt von Multiplikatoren, die die Idee des dezentralen, freien und offenen Netzwerkes weitertragen. Multiplikatorinnen wie Du und ich und unsere Freunde und deren Freundinnen und die Freundinnen der Freunde der Freunde... Sobald eine kritische Nutzerinnenmasse erreicht ist, können wir gemeinsam viel bewegen. Denn wenn wir nicht mal langsam „in die Pötte kommen“, wird Facebook nur noch dreister unsere Daten und die unserer Freundinnen und Freunde (oder Bekannten) vermarkten.

Dies ist ein langfristiges Projekt und uns ist klar, dass es Zeit, Arbeit und Geduld erfordert, bis wir an einem Punkt angelangt sind, an dem wir tatsächlich etwas bewegen können. Facebook hat nach eigenen Angaben mehr als 900 Millionen Nutzer weltweit und wächst stetig weiter. Auch in anderen Ländern wächst dabei der Unmut über einen Konzern, der versucht, Gesetzen zum verantwortungsbewussten Umgang mit seinen Nutzerdaten aus dem Weg zu gehen. Daher arbeiten wir mit internationalen Kooperationspartnern zusammen, um gemeinsam eine Lösung zu finden die nicht nur im deutschsprachigen Raum, sondern auch weltweit funktioniert. Damit der Social Swarm möglichst bald in Richtung dezentrale Freiheit aufbrechen kann, brauchen wir Menschen, die unseren Traum von einem freien öffentlichen Raum im Netz teilen und sich dem Social Swarm anschließen.

Der FoeBuD aus Bielefeld hat die Initiative übernommen, die vielen Fäden zu bündeln und zu moderieren. Das läuft dabei derzeit hauptsächlich über die englischsprachige Mailingliste und eine Entscheidungsplattform namens „Liquid Feedback“. Hier kommt der Social Swarm zusammen, um potentielle Kandidaten für ein neues dezentrales Netzwerk ausfindig zu machen und Strategien zu diskutieren. Den Stand der Debatte kann man jederzeit auf der Homepage und im öffentlichen Wiki nachlesen. Wer mitmachen möchte beim Vorbereiten des Wechsels, ist eingeladen, seine Kompetenzen mit einzubringen.

Link zur Homepage:
https://www.socialswarm.net
Link zum Wiki:
https://wiki.socialswarm.net[

1 Laudatio von Rena Tangens anläßlich der 11. Verleihung der BigBrotherAwards: http://www.bigbrotherawards.de/2011/.comm1

2 Tim Berners-Lee zur Gefahr Facebook: http://www.zdnet.de/news/41540964/web-erfinder-tim-berners-lee-warnt-vor-facebook.htm)

Dr. jur. Georgios Samartzis

Sozialdatenschutz bei inneradministrativen Prozessen am Beispiel des Psychologischen Dienstes der Bundesagentur für Arbeit

I. Einleitung

Die Frage, ob Arbeitsuchende oder Arbeitslose über die notwendigen mentalen und sozialen Voraussetzungen für die Besetzung eines bestimmten, freien Stellenangebots verfügen, lässt sich in der Praxis der Arbeitsverwaltung zuweilen nur durch Einholung von fachlicher Expertise des Psychologischen Dienstes der Bundesagentur für Arbeit klären. Der Psychologische Dienst ist neben dem Ärztlichen Dienst der zweite Fachdienst innerhalb der Bundesagentur, welcher dem operativen Bereich mit Rat und Tat zur Seite steht, wenn es um die Klärung der Einsatzfähigkeit von Arbeitsuchenden oder Arbeitslosen geht. Auf lokaler Ebene sind die Psychologischen Dienste den örtlichen Arbeitsagenturen angegliedert. Die Arbeitsvermittler haben bei der Einschaltung des Psychologischen Dienstes den Sozialdatenschutz zu beachten. Im Folgenden soll ein Überblick über die hierfür maßgeblichen Aspekte erfolgen.

II. Datenerhebung

Eine Erhebung von Sozialdaten im Sinne des zweiten Kapitels des SGB X ist bei der Einschaltung des Psychologischen Dienst gemäß § 67a Abs. 1 SGB X immer dann zulässig, wenn deren Kenntnis zur Aufgabenerfüllung der Bundesagentur für Arbeit erforderlich ist. Das Einverständnis des Betroffenen für eine Beauftragung des Psychologischen Dienstes ist primär durch den Arbeitsvermittler einzuholen. Lediglich in Ausnahmefällen kann das Einverständnis durch einen Mitarbeiter des Psychologischen Dienstes eingeholt werden. Dies ist auf dem Befundbogen zu vermerken.

Da Sozialdaten grundsätzlich beim Betroffenen selbst zu erheben sind (§ 67a Abs. 2 SGB X), können entsprechende Daten bei Dritten (z. B. Erziehungsberechtigten, Ehe- und Lebenspartnern, sonstige Familienangehörigen) nur dann erhoben werden, wenn der Betroffene dem zugestimmt hat und

die Datenerhebung bei einer dritten Person aus fachlichen Gründen notwendig ist. Hinsichtlich der Zustimmung, welche stets schriftlich einzuholen ist, soll der Betroffene auf die Freiwilligkeit der Abgabe, den Frageninhalt sowie die fachlichen Gründe hingewiesen werden.

Sofern Voruntersuchungen (Befundberichte und Gutachten) zu Begutachtungszwecken beigezogen werden, ist, soweit es sich nicht um Unterlagen anderer Sozialleistungsträger handelt, vorab vom Betroffenen eine schriftliche Schweigepflichtentbindungserklärung einzuholen.

III. Aufbewahrung von Sozialdaten

Sozialdaten, welche im Psychologischen Dienst gespeicherten werden, sind gegen unbefugte Einsichtnahme und Mitnahme zu sichern. So sind etwa während der Dienststunden die Diensträume beim Verlassen abzusperren und Computer gegen unerlaubten Zugriff zu sichern. Für den Fall, dass sich ein Drucker in einem Raum befindet, in dem kein Mitarbeiter des Psychologischen Dienstes seinen Arbeitsplatz hat, darf diese Räumlichkeit während des Druckbetriebs nur den Mitarbeitern des Psychologischen Dienstes offenstehen.

Sämtliche Unterlagen mit Sozialdaten sind nach Dienstschluss gemäß den folgenden Sicherheitsmaßnahmen aufzubewahren: Dem Reinigungspersonal und anderen, mit der Sache nicht befassten Personen darf keine Einsicht in Unterlagen möglich sein. Gutachten und Befundunterlagen sind in abschließbaren Schränken, Schreibtischen oder anderen Behältnissen aufzubewahren. In Archivräumen kann dann von dieser Sicherung abgesehen werden, wenn diese einerseits mit Sicherheitsschlössern verschließbar sind, und wenn andererseits gewährleistet ist, dass Personen, die nicht dem Psychologischen Dienst angehören, keinen Zugang zu diesen Räumen haben.

Der Psychologische Dienst leitet Unterlagen, die Sozialdaten enthalten, stets in Verschlussmappen weiter. Für den postalischen Versand von Einladungen oder anderen Schriftstücken an die Arbeitsuchenden oder Arbeitslosen werden Briefumschläge der jeweiligen Agentur für Arbeit ohne einen Hinweis auf den Psychologischen Dienst auf dem Couvert verwendet.

IV. Grundsätze im Umgang mit Sozialdaten

1. Vermeidung einer strafrechtlich sanktionierten Offenbarung (§ 203 Strafgesetzbuch)

Ein Psychologe macht sich gemäß § 203 Strafgesetzbuch strafbar, wenn er, ohne hierzu vom Betroffenen autorisiert zu sein, ein zu dessen persönlichem Lebensbereich gehörendes Geheimnis offenbart, das ihm in seiner Eigenschaft als Psychologe anvertraut oder sonst bekannt geworden ist. Diese Norm gilt nicht nur für die Psychologen im Psychologischen Dienst, sondern vielmehr für alle Mitarbeiter dieses Dienstes, auch für nur temporär im Psychologischen Dienst tätige Personen, wie etwa Praktikanten oder Hospitanten (§ 203 Abs. 3 Satz 2 StGB). In der Praxis wird davon ausgegangen, dass es sich bei allen dem Psychologischen Dienst bekannt gewordenen Sozialdaten um Geheimnisse im Sinne des § 203 StGB handelt.

Der Begriff der „Offenbarung“ kann als Mitteilen eines Geheimnisses an einen Dritten definiert werden – auch durch schlüssiges Verhalten oder durch Unterlassen der datenschutzgerechten Aufbewahrung von Sozialdaten – durch welches dieser Kenntnis erhält über ihm noch nicht, nicht in dem Umfang, nicht in dieser Form oder nicht sicher bekannte Tatsachen.

Die Befugnis zur Offenbarung liegt immer dann vor, wenn der Arbeitsuchende oder Arbeitslose in die Offenbarung eingewilligt hat oder eine Offenbarung, etwa strafrechtlich nach §§ 32, 34 oder 138 StGB geboten oder gerechtfertigt ist.

Die Wirksamkeit der Einwilligung, ebenso wie eine Verweigerung der Zustimmung zur Weitergabe von Daten, hängt stets von der Einsichts- und Urteilsfähigkeit des Betroffenen ab.

Hervorzuheben ist in diesem Kontext, dass grundsätzlich kein Offenbarungsanspruch von Eltern minderjähriger Betroffener gegenüber einem Psychologen der Bundesagentur existiert. Allerdings kann nach den Grundsätzen der Pflichtenkollision in Ausnahmefällen eine Offenbarungspflicht gegenüber den Eltern bejaht werden, wenn die bei einer Untersuchung bekannt gewordenen Geheimnisse im Hinblick auf ihre Tragweite sowie unter Berücksichtigung der geistigen Reife des Betroffenen eine Offenbarung im Sinne des elterlichen Personensorgerechts notwendig machen. Dasselbe gilt gegenüber Betreuungspersonen nach § 1902 BGB. Im Gegensatz zu Eltern von minderjährigen Betroffenen kommt einem Betreuer die Rechtsstellung eines gesetzlichen Vertreters aber nur insoweit zu, als er diese zur Erfüllung der ihm übertragenen Aufgaben benötigt.

Bei der Nutzung und Übermittlung von Sozialdaten ist stets § 67b Abs. 1 SGB X zu beachten, wonach von einer Zulässigkeit der Nutzung und Übermittlung von Sozialdaten immer dann ausgegangen werden kann, wenn eine Einwilligung des Betroffenen vorliegt. Liegt eine Einwilligung des Betroffenen in die Offenbarung vor, ist damit zugleich auch seine Einwilligung zur Nutzung und Übermittlung der Sozialdaten gegeben.

2. Datennutzung (§ 67c Abs. 1 und 2 SGB X)

Innerhalb der Bundesagentur für Arbeit stellt die Weitergabe von Gutachten oder anderer im Psychologischen Dienst gespeicherter Sozialdaten eine zulässige Nutzung von Sozialdaten gemäß § 67c Abs. 1 SGB X dar.

Bei den durch den Psychologischen Dienst erbrachten Dienstleistungen „Berufswahltest“, „Studienfeldbezogene Beratungstestserie“, „Psychologische Auswahlbegutachtung“, „Psychologische Kurzbegutachtung“, „Psychologische Begutachtung“, „Psychologische Begutachtung von Sinnesbeeinträchtigten“ und „Gemeinsame Fallbearbeitung“ kann im Allgemeinen von einer stillschweigenden Einwilligung des Arbeitsuchenden oder Arbeitslosen zur Offenbarung ausgegangen werden. Für den Fall, dass sich diese Annahme als falsch erweisen sollte, erläutert der Psychologe den Zweck, die Notwendigkeit sowie die Rechtsgrundlage der psychologischen Dienstleistung und erbittet die Einwilligung zur Offenbarung. Erteilt der Arbeitsuchende oder Arbeitslose

die erbetene Einwilligung nicht oder zieht er sie zurück, ist die entsprechende Dienstleistung abzubrechen und dem für den Betroffenen zuständigen Arbeitsvermittler als ursprünglichen Auftraggeber mitzuteilen, dass die jeweilige Serviceleistung des Psychologischen Dienstes aufgrund der fehlenden Mitwirkung des Betroffenen nicht durchgeführt werden konnte.

Vor Darbietung der Dienstleistung „Psychologischen Beratung" weist der mit der Beratung beauftragte Psychologe den Kunden ebenfalls auf die Freiwilligkeit der Inanspruchnahme hin und dokumentiert dies auf dem Befundbogen. Ist ein Arbeitsuchender oder Arbeitsloser zu einer „Psychologischen Beratung" nicht bereit, wird diese Serviceleistung ebenfalls nicht begonnen, beziehungsweise abgebrochen.

Sozialdaten, die der Psychologische Dienst im Rahmen seiner Fallarbeit erhebt, dürfen nur an Mitarbeiter der Bundesagentur für Arbeit weitergegeben werden, die mit der Sache befasst sind. Hierzu gehören neben dem veranlassenden Mitarbeiter (in der Regel der Arbeitsvermittler) und dem Arzt der Agentur für Arbeit auch die zuständigen Vorgesetzten, die zur Entscheidung im Einzelfall die entscheidungsbegründenden Unterlagen benötigen. Daneben gehören auch Mitarbeiter dazu, die für die Zu- und Mitarbeit im Psychologischen Dienst verantwortlich sind (Fachkräfte und Assistenzkräfte).

Eine Weitergabe von Befundunterlagen an außerhalb des Psychologischen Dienstes tätige Mitarbeiter der Bundesagentur für Arbeit findet allerdings nicht statt. Zudem ist es diesen Mitarbeitern auch nicht gestattet, von sich aus in diese Unterlagen Einsicht zu nehmen. Davon ausgenommen sind die Ärzte der Agentur für Arbeit, welche in die Befundunterlagen Einsicht nehmen dürfen, soweit der Betroffene schriftlich in die Offenbarung eingewilligt hat, sowie Mitarbeiter der Bundesagentur für Arbeit, welche im Rahmen ihrer Aufgabenerledigung für die Datenübermittlung an Gerichte im Zusammenhang mit einer sozialen Aufgabenerledigung zuständig sind (s. hierzu unten IV. 3. c).

Im Kontext regelmäßiger Prüfungen durch die Zentrale und durch die Regionaldirektionen der Bundesagentur für Arbeit auf Ebene der lokalen Arbeitsagenturen sowie im Rahmen der Führung, Steuerung und Fachaufsicht wird darüber hinaus den mit diesen Aufgaben betrauten Führungskräften und Mitarbeitern unbeschränkte Einsicht in Unterlagen zugestanden, in dem Sozialdaten vermerkt sind. Dies gilt ebenso für Mitarbeiter mit Prüfungsaufgaben beim Bundesministerium für Arbeit und Soziales als Rechtsaufsichtsbehörde wie für den Bundesbeauftragten für den Datenschutz und den Bundesrechnungshof.

Eine Besonderheit gilt für Personen, die das Dienstleistungsspektrum des Psychologischen Dienstes nutzen und zugleich an einem Zeugenschutzprogramm partizipieren. In diesem Fall erhält der Zeugenschutzbeauftragte der jeweiligen Dienststelle alle Unterlagen der geschützten Person zugeleitet. Die in den IT-Verfahren der Bundesagentur gespeicherten Daten des Betroffenen werden umgehend gelöscht. Die Fallunterlagen werden in Papierform in abgeschlossenen Schränken gesondert aufbewahrt.

3. Datenübermittlung (§§ 67d ff. SGB X)

a) Grundsatz

Eine Übermittlung findet ausschließlich an die unter lit. b) bis j) angeführten Personen und Institutionen statt. Eine Weitergabe an andere Stellen ist selbst für den Fall, dass der Betroffene dies ausdrücklich wünscht, nicht statthaft. Der Psychologische Dienst führt zu keinem Zeitpunkt eine Übermittlung an einen aktuellen oder potenziellen Arbeitgeber des Betroffenen durch.

Schriftwechsel und Aktenvermerke, die im Rahmen der Erbringung von psychologischen Dienstleistungen anfallen, werden zu den Fall-Akten genommen. Falls eine Offenbarung und Übermittlung von Sozialdaten an Außenstehende erfolgt, soll diese durch einen Psychologen der Agentur für Arbeit durchgeführt werden, und zwar möglichst durch denjenigen, welcher den jeweiligen Betroffenen begutachtet oder beraten hat.

Ein postalischer Versand von Unterlagen erfolgt stets in einem verschlossenen Couvert mit einem Verschlussstreifen, auf dem ausdrücklich vermerkt wird, von wem der Umschlag zu öffnen ist. Eine Herausgabe von Test- und Befundbögen findet – auch in Form von Kopien – nicht statt.

b) Übermittlung an Ärzte und an Angehörige von Heil- und Sozialberufen

An Ärzte können Gutachten und Untersuchungsbefunde übermittelt werden, wenn sie für die Behandlung des Betroffenen von Bedeutung sind und dieser hierzu eingewilligt hat (§§ 101 SGB X). Auch an die Angehörigen von Heil- oder Sozialberufen sind Gutachten, welche im Rahmen der Fallarbeit erhoben wurden, zu übermitteln, sobald der Betroffene eingewilligt hat und die Übermittlung aus Sicht des Psychologischen Dienstes als sachdienlich eingestuft wird.

c) Übermittlung an Gerichte im Zusammenhang mit einer sozialen Aufgabenerledigung

Eine Herausgabe von Unterlagen des Psychologischen Dienstes an die Sozialgerichte oder sonstigen Gerichte im Kontext der Erledigung von sozialen Aufgaben durch die Bundesagentur für Arbeit findet im Rahmen des § 69 Abs. 1 Nr. 1 und Nr. 2 SGB X durch die für das laufende Verwaltungsverfahren zuständige Organisationseinheit statt. Im Allgemeinen handelt es sich bei dieser Organisationseinheit um das Team „Widerspruchsstelle/SGG", welches in jeder Arbeitsagentur vorhanden ist. Ein etwaiger Widerspruch des Betroffenen gegen eine derartige Übermittlung ist von dieser Organisationseinheit zu berücksichtigen.

d) Weitergehende Übermittlung an Gerichte

Die Herausgabe von Unterlagen des Psychologischen Dienstes an Gerichte im Rahmen von Verfahren, die nicht im Zusammenhang mit der Erfüllung von sozialen Aufgaben durch einen Sozialleistungsträger stehen, kann nur auf Anforderung des Gerichts und nur mit schriftlicher Einwilligung des Betroffenen erfolgen.

e) Übermittlung an Sozialleistungsträger und Jugendämter

Beantragen andere Sozialleistungsträger sowie Jugendämter zur Erfüllung der ihnen nach dem Sozialgesetzbuch übertragenen Aufgaben (einschließlich damit zusammenhängender Sozialgerichts- oder Strafverfahren) die Übermittlung von Ergebnissen aus einer psychologischen Begutachtung, so ist von diesen Stellen zunächst das Vorliegen der Voraussetzungen des § 69 Abs. 1 Nr. 1 SGB X darzulegen sowie eine Erklärung abzugeben, dass der Betroffene vorab auf sein Widerspruchsrecht nach § 76 Abs. 2 SGB X hingewiesen worden ist und davon keinen Gebrauch gemacht hat. Wie bei den vorgenannten Fallkonstellationen auch, erfolgt eine Übermittlung von Gutachten durch den Psychologischen Dienst und nicht durch eine andere Organisationseinheit innerhalb der Arbeitsagentur. Eine Herausgabe von Befundunterlagen erfolgt im Zusammenhang mit Sozialgerichts- oder Strafverfahren nur an das zuständige Gericht, nicht jedoch unmittelbar an Sozialleistungsträger.

f) Übermittlung an einen Träger von berufsfördernden Maßnahmen

An einen Träger von berufsfördernden Maßnahmen im Rahmen der Aufgabenerfüllung nach dem SGB III können Kopien von Gutachten weitergegeben werden, sofern diese Weitergabe aus Sicht des Psychologischen Dienstes sachdienlich erscheint und der Betroffene schriftlich in die Übermittlung eingewilligt hat. Es findet allerdings generell keine Herausgabe von Befundunterlagen an einen Träger von berufsfördernden Maßnahmen statt.

g) Übermittlung an Träger von Maßnahmen zur Rehabilitation

An einen Träger von Maßnahmen zur Rehabilitation können durch die auftragserteilende Stelle (in der Regel der Arbeitsvermittler) Kopien der vorhandenen Gutachten übermittelt werden, sofern der Betroffene seine schriftliche Einwilligung hierzu gegeben hat. Die Einwilligung wird im Rahmen des Verwaltungsverfahrens durch die zuständige Fachkraft eingeholt. Wie bei der zuvor genannten Übermittlungsart ist auch hier eine Herausgabe von Befundunterlagen an den Träger nicht statthaft.

h) Übermittlung an die Polizeiverwaltung

Die Bundesagentur ist gemäß § 68 SGB X gegenüber den Behörden der Polizeiverwaltung zur Offenbarung verpflichtet. Diese Offenbarung beschränkt sich allerdings auf die Daten „Name“, „Geburtsort“, „Anschrift“ und „Arbeitgeber“. Ein Hinweis darauf, dass jemand für eine psychologische Dienstleistung der Arbeitsagentur vorgesehen ist, sowie die Bekanntgabe des entsprechenden Termins, würde einen Verstoß gegen § 203 StGB darstellen. Die Offenbarung eines solchen Geheimnisses wäre nur dann zulässig, wenn ein rechtfertigender Notstand nach § 34 StGB vorliegen würde. Allerdings ist von der Polizeibehörde eine richterliche Anordnung vorzulegen, aus der ein rechtfertigender Notstand hervorgeht.

i) Übermittlung zum Zwecke der wissenschaftlichen Forschung

Innerhalb der Arbeitsverwaltung entscheidet das sogenannte „Service-Haus“ in Absprache mit dem Bereich „VA 2 (Datenschutz / Justiziariat)“ der Zentrale der Bundesagentur für Arbeit, ob Daten zu Forschungszwecken, welche einen statistischen Bezug aufweisen, übermittelt werden dürfen. Bei sonstigen Forschungsvorhaben, ist für die Entscheidung das Institut für Arbeitsmarkt- und Berufsforschung der Bundesagentur für Arbeit (IAB) zuständig.

Die „Wissenschaftlichkeit“ stellt in diesem Kontext einen unbestimmten Rechtsbegriff dar, für den keine genaue Definition existiert. In der Praxis wird als maßgebliches Kriterium die Frage herangezogen, ob es sich um einen ernsthaften Erkenntnisprozess handelt. Ein reines Archivierungsinteresse würde demnach nicht hierunter fallen. Bei der Anfertigung einer Diplomarbeit oder einer Promotion wird hingegen ein ernsthafter Erkenntnisprozess im Allgemeinen unterstellt, wobei das Thema der Arbeit einen erkennbaren Bezug zum Sozialleistungsbereich haben sollte.

j) Übermittlung an den Petitionsausschuss des Deutschen Bundestages

Bei einer Übermittlung an den Petitionsausschuss des Deutschen Bundestages sowie an andere Personen oder Stellen des persönlichen Vertrauens des Betroffenen, insbesondere an politische Mandatsträger oder an Medien gilt, dass eine Herausgabe von Sozialdaten immer nur mit Einwilligung des Betroffenen möglich ist. Bei der Prüfung der Frage, ob die Übermittlung einer Kopie des Gutachtens für das Anliegen des Betroffenen erforderlich ist, wird der Psychologische Dienst vorab vom operativen Bereich konsultiert.

V. Das Recht auf Akteneinsicht gemäß § 25 SGB X

Eine an einem Sozialverwaltungsverfahren beteiligte Person besitzt nach § 25 SGB X das Recht auf Akteneinsicht. Verlangt eine vom Psychologischen Dienst untersuchte oder beratene Person ausdrücklich Akteneinsicht nach § 25 SGB X, so wird sie an diejenige Stelle verwiesen, die ursprünglich die Einschaltung des Psychologischen Dienstes veranlasst hat, in der Regel also an den Arbeitsvermittler. Ihm obliegt sodann die Entscheidung, ob die Voraussetzungen für eine Akteneinsicht nach § 25 SGB X gegeben sind. Er unterrichtet anschließend den Psychologischen Dienst über seine Entscheidung.

Sind die Voraussetzungen für eine Akteneinsicht gegeben, vermittelt der zuständige Psychologe der Agentur für Arbeit dem Betroffenen den Inhalt des Gutachtens sowie, falls vorhanden, den Inhalt der Befundunterlagen. Er gewährt dem Betroffenen die Einsicht in seine Unterlagen sowie in die maßgeblichen Sozialdaten, die in den lT-Anwendungen der Bundesagentur gespeichert sind. Dabei darf der Betroffene keine Einsicht in Daten anderer Personen erhalten. Auf Wunsch erhält er eine Kopie des Gutachtens. Soweit der Betroffene auch die Befundunterlagen einer psychologischen Test-Untersuchung wünscht, erhält er Kopien seines Profilbogens und, falls vorhanden, Kopien der Befundübersicht.

Beantragt ein minderjähriger Betroffener Akteneinsicht, so ist zwischen seinem Recht auf Akteneinsicht

und der ihm gegenüber bestehenden Fürsorgepflicht der Arbeitsagentur abzuwägen. Der zuständige Psychologe der Agentur für Arbeit entscheidet, ob durch eine Akteneinsicht die Entwicklung und Entfaltung der Persönlichkeit des Minderjährigen beeinträchtigt werden kann. Sollte dies der Fall sein, wird der Antrag des minderjährigen Betroffenen auf Akteneinsicht abgelehnt. Fordert der Minderjährige die Akteneinsicht in Begleitung eines Erziehungsberechtigten und willigt dieser in die Akteneinsicht ein, so wird dem Betroffenen trotz eventueller Bedenken auf Seiten des Psychologischen Dienstes die Akteneinsicht gewährt.

In den IT-Verfahren der Bundesagentur wird durch den Psychologischen Dienst vermerkt, dass dem Beteiligten (oder seinem Bevollmächtigten) der Inhalt eines Gutachtens vermittelt wurde, er nach § 25 SGB X Akteneinsicht erhalten hat und welche Kopien ihm dabei ausgehändigt worden sind.

VI. Auskunftsrecht gemäß § 83 SGB X

Gemäß § 83 Abs. 1 SGB X ist den Arbeitsuchenden oder Arbeitslosen Auskunft über die zu ihrer Person gespeicherten Daten zu erteilen. Dabei bestimmt die Bundesagentur als speichernde Stelle nach pflichtgemäßen Ermessen das Verfahren und damit auch die Form der Auskunftserteilung.

Auf Wunsch wird dem Betroffenen durch den zuständigen Agentur-Psychologen Einsichtnahme in die zu seiner Person gespeicherten Daten, wie etwa Gutachten und Befundunterlagen sowie die im IT-Verfahren gespeicherten Sozialdaten gewährt. Die Gutachten des Psychologischen Dienstes gelten als interne Arbeitsmittel, welche ausschließlich der fachlichen Informationsweitergabe an die Vermittlungsfachkräfte dienen. Der Betroffene kann allerdings auf Wunsch eine Kopie des Gutachtens erhalten, wenn unter Berücksichtigung aller Umstände des Einzelfalls eine missbräuchliche Verwendung ausgeschlossen werden kann.

Gemäß § 13 SGB X kann eine Auskunft nach § 83 SGB X an einen Bevollmächtigten des Betroffenen erteilt werden, wenn dessen Bevollmächtigung auch eine Auskunftserteilung umfasst.

Beantragt ein Arbeitsuchender oder Arbeitsloser in Begleitung eines Dritten die Auskunftserteilung, so wird vom Psychologen der Agentur für Arbeit zunächst geklärt, ob der Betroffene ohne Zwang in eine Offenbarung an den Dritten eingewilligt hat. Existieren hieran Zweifel, wird der Dritte von einer Einsichtnahme ausgeschlossen.

In den IT-Verfahren der Bundesagentur wird nach der Auskunftserteilung stets gespeichert, dass diese stattgefunden hat sowie welche Kopien oder Ausdrucke ausgehändigt worden sind. Zudem werden die Personalien eines eventuell vorhandenen Bevollmächtigten oder eines den Betroffenen begleitenden Dritten, ggf. die Einwilligung eines Erziehungsberechtigten, und falls erfolgt, die Ablehnung eines Antrags vermerkt. Die Kopie einer Vollmacht wird zu den Fall-Akten genommen.

VII. Weitere Rechte des Beteiligten

1. Grundsatz

Arbeitsuchende oder Arbeitslose können Sozialdaten löschen, sperren oder berichtigen lassen. Die entsprechende Rechtsgrundlage hierfür findet sich in § 84 SGB X.

Eine Löschung, Sperrung oder Berichtigung von Sozialdaten erfolgt durch den Psychologen der Agentur für Arbeit, welcher den Kunden begutachtet oder beraten hat. Dieser Psychologe benachrichtigt im Falle einer Löschung, Sperrung oder Berichtigung hierüber auch alle Stellen und Personen, an die der Psychologische Dienst Sozialdaten weitergegeben oder übermittelt hat.

Eine Berichtigung, die keine fachliche oder rechtliche Relevanz besitzt, kann auch von jedem anderen Mitarbeiter des Psychologischen Dienstes durchgeführt werden.

Ein ablehnender Bescheid über einen Antrag auf Berichtigung, Sperrung oder Löschung von Sozialdaten wird hingegen vom unmittelbaren Fachvorgesetzten des begutachtenden oder beratenden Psychologen erstellt, in der Regel also vom leitenden Psychologen des örtlichen Psychologischen Dienstes. Der Ablehnungsbescheid wird mit einer Rechtsbehelfsbelehrung versehen.

2. Recht auf Datenlöschung

Eine Datenlöschung nach § 84 Abs. 2 SGB X erfolgt mittels Schwärzen von Texten, der Vernichtung der gesamten Akte oder durch eine Löschung in den entsprechenden IT-Anwendungen der Bundesagentur. Bei einer Schwärzung wird die Notiz „gelöscht“ vermerkt, sowie das Handzeichen nebst Datum hinzugefügt. Im Falle einer kompletten Löschung der Sozialdaten eines Arbeitsuchenden oder Arbeitslosen wird hierüber ein Vermerk angefertigt, soweit die Löschung vor Ablauf der Aufbewahrungszeit stattgefunden hat.

3. Recht auf Sperrung

Bei der Sperrung von Sozialdaten gemäß § 84 Abs. 3 SGB X werden die zu sperrenden Daten mit der Notiz „Diese Daten sind gesperrt“ versehen. Zudem ist auch hier noch das Handzeichen nebst Datum hinzuzufügen.

4. Recht auf Berichtigung

Ebenso ist eine rechtlich oder fachlich relevante Berichtigung nach § 84 Abs. 1 SGB X mit einer Notiz („Berichtigt“) und mit dem Handzeichen nebst Datum zu versehen. Bestreitet der Betroffene die Richtigkeit von Sozialdaten und lässt sich im Ergebnis weder eine Richtigkeit noch eine Unrichtigkeit feststellen, werden die bestrittenen Daten mit einer Notiz („Diese Daten werden bestritten. Ihre Richtigkeit oder Unrichtigkeit lässt sich nicht feststellen.“) versehen. Zudem wird auch in diesem Fall die Notiz mit dem Handzeichen sowie dem Datum ergänzt. Bestrittene Daten dürfen nur mit einem Hinweis hierauf genutzt und übermittelt werden.

VIII. Partizipation weiterer Personen

Wie bereits dargelegt, können Erziehungsberechtigte, Ehe- und Lebenspartner, Familienangehörige sowie Vertrauenspersonen an einem Gespräch des Arbeitsuchenden oder Arbeitslosen mit einem Psychologen des Psychologischen Dienstes teilnehmen, soweit der Betroffene dies ausdrücklich wünscht und keine fachlichen Einwände hiergegen existieren.

Die Teilnahme an einer psychologischen Untersuchung oder Beratung kann anderen Mitarbeitern der Bundesagentur für Arbeit nach vorhergehender Unterrichtung des Kunden gestattet werden.

Psychologen, welche der Bundesagentur für Arbeit nicht angehören, sowie Studierenden der Psychologie kann eine Teilnahme gestattet werden, wenn dies für ihre Ausbildung oder Weiterbildung dienlich ist oder im Interesse der Bundesagentur für Arbeit liegt. Allerdings ist auch hier vorab die Einwilligung des Kunden einzuholen. Die externen Teilnehmer werden vom Psychologischen Dienst auf ihre Schweigepflicht nach § 203 StGB hingewiesen.

IX. Umgang mit personenbezogenen Daten von Einstellungsbewerbern

Für den Fall, dass der Psychologische Dienst bei der Auswahl von Bewerbern der Bundesagentur für Arbeit in deren Eigenschaft als Arbeitgeber tätig wird, kommen hinsichtlich des Datenschutzes nicht die Bestimmungen zum Schutz der Sozialdaten nach dem Sozialgesetzbuch zur Anwendung. Vielmehr sind hier die Datenschutzbestimmungen des Bundesdatenschutzgesetzes sowie weitere spezielle Regelungen, wie etwa die §§ 106ff. Bundesbeamtengesetz und die Personalaktenrichtlinie der Bundesagentur für Arbeit nebst den entsprechenden Durchführungshinweisen zu beachten. Allerdings erfolgt der Umgang mit und die Aufbewahrung von personenbezogenen Daten von Bewerbern analog den Regelungen für Sozialdaten.

In der Praxis werden psychologische Stellungnahmen und Testergebnisse, die als Grundlage für Personalentscheidungen dienen, offen in der Personalakte abgeheftet. Soweit allerdings über diese personalentscheidungsrelevanten Stellungnahmen hinaus vom zuständigen Psychologen fachliche Detailaussagen getroffen wurden, werden die entsprechenden Unterlagen hierzu im Psychologischen Dienst aufbewahrt.

Generell in einem verschlossenen Umschlag werden diejenigen psychologischen Unterlagen zur Personalakte genommen, die im Rahmen der Prüfung und Entscheidung über die Dienstfähigkeit oder im Zusammenhang mit der Prüfung der Erwerbsfähigkeit von Beschäftigten der Bundesagentur angefallen sind.

Verlangt ein nicht eingestellter Bewerber vom Psychologischen Dienst eine Auskunft über die zu seiner Person gespeicherten Daten, wird ebenso verfahren wie bei Arbeitsuchenden oder Arbeitslosen, welche eine Auskunft nach § 83 SGB X verlangen. Allerdings wird dem Betroffenen grundsätzlich erst nach Abschluss des Auswahlverfahrens die gewünschte Auskunft gegeben. Eine Löschung, Sperrung oder Berichtigung von personenbezogenen Daten erfolgt ebenfalls analog zu den Regelungen für Sozialdaten.

X. Fazit

Auch bei administrativen Prozessen „innerhalb“ eines Sozialleistungsträgers besitzt der Schutz von Sozialdaten einen hohen Stellenwert. Die Interaktion zwischen dem operativen Bereich „Arbeitsvermittlung“, dem „Internen Personalbereich“ sowie dem Fachdienst „Psychologischer Dienst“ der Bundesagentur für Arbeit ist in diesem Zusammenhang von klaren Vorgaben geprägt. Die oben dargelegten Ausführungen zeigen, dass der Sozialdatenschutz nicht nur beim eigentlichen „Kerngeschäft“ der Bundesagentur für Arbeit und bei der unmittelbaren Zusammenarbeit mit den Arbeitsuchenden und Arbeitslosen eine wichtige Rolle spielt. Auch beim Einschalten subsidiärer Fachdienste oder im „Internen Personalbereich“ sind die datenschutzrechtlichen Vorgaben klar geregelt und deren Nachhaltung somit objektiv überprüfbar.



BITTE TERMIN VORMERKEN!

Die Deutsche Vereinigung für Datenschutz e.V. wird auch in diesem Jahr wieder ein Expertengespräch im Europäischen Parlament durchführen.

Am 04.09.2012 werden wir mit Parlamentariern und allen Interessierten in Brüssel die Auswirkungen der Europäischen Datenschutzgrundverordnung diskutieren.

Als parlamentarische Gastgeberin wird in diesem Jahr Frau Birgit Sippel von der sozialdemokratischen Fraktion des EP fungieren.

Jan Kuhlmann

EGK – Too big to fail? Ein Zwischenbericht.

1. Einleitung

Das Projekt EGK stammt aus den 1980er Jahren, die jetzige Krankenversichertenkarte (KVK) sollte schon 1992 zur EGK weiterentwikkelt werden, mit den heute bekannten Anwendungen – ein Großprojekt auf Grundlage proprietärer, patentgeschützer Hardware (Näheres zur Geschichte in der Broschüre des Forums InformatikerInnen für Frieden und Gesellschaftliche Verantwortung, 2. Auflage, Seite 6-17: http://fiff.de/publikationen/broschueren/20110620_FIfF-egk_digitaleVersionV2.pdf/view). Seit 2004 steht im Gesetz, dass die EGK ab 2006 verbindlich ist. Zur Zeit wird sie „ausgerollt“. Nach neuesten gesetzlichen Vorgaben sollten letztes Jahr 10 % der Versicherten die Karte erhalten, dieses Jahr soll die Quote auf 70 % steigen. Krankenkassen, die nicht spuren, erhalten weniger Geld. Eine wirksame Drohung, da die Kassen nur noch aus dem staatlichen Gesundheitsfond Geld erhalten. Die meisten Abgeordneten, die dieser gesetzlichen Erpressung zustimmten, haben das gar nicht mitbekommen. Für die Wirksamkeit kommt es darauf nicht an.

Immer wieder hört man von Versicherten, dass sie die EGK bekommen haben, auch wenn offenbar weder letztes Jahr 10 % erreicht wurden noch dieses Jahr 70 % erreicht werden, da die größten Kassen sich zurückhalten. Zuerst wird man aufgefordert, ein Bild einzuschicken, dann wird es auf die EGK gedruckt und schließlich bekommt man sie. Die EGK kostet die Krankenkassen ca. zehnmal soviel wie die KVK und braucht neue Lesegeräte, die parallel in den Arztpraxen, Apotheken, Krankenhäusern verteilt wurden. Auch das wird von den Krankenkassen bezahlt, also von uns allen.

Die EGK ist die Eintrittskarte für eine neue technische Infrastruktur im Gesundheitswesen, genannt „Telematik-Infrastruktur“. Diese wird organisiert von der Gematik in Berlin, einer GmbH, in der die Krankenkassen, Ärzte, Krankenhäuser, sowie IT-Industrie und Datenschützer vertreten sind. Die Karte verhält sich zur Infrastruktur wie die Spitze des Eisbergs zum Eisberg – sie bildet die sichtbaren 10 %. Darunter liegt eine Infrastruktur, die zehntausende Rechner aller Institutionen des Gesundheitswesens über das Internet miteinander verknüpft, natürlich verschlüsselt, ausgelegt allerdings nicht für Röntgenbilder oder Abbildungen von EKGs. Es geht ausschließlich um Verwaltungs- und Abrechnungsdaten.

In Großbritannien wurde letztes Jahr ein vergleichbares Projekt storniert, das jahrelang nicht von der Stelle gekommen war (http://www.heise.de/newsticker/meldung/Britischer-Gesundheitsdienst-kippt-milliardenschweres-IT-Projekt-1349236.html). Da hierzulande nur Piraten und Linke gegen die EGK sind, wird sich das Projekt noch lange dahinschleppen.

2. Die EGK als Thema für Transparency International

„Stiehlt einer ein Geldstück, dann hängt man ihn. Wer öffentliche Gelder unterschlägt, wer durch Monopole, Wucher und tausenderlei Machenschaften und Betrügereien noch so viel zusammenstiehlt, wird unter die vornehmen Leute gerechnet“ (Erasmus von Rotterdam).

Auf den ersten Blick scheint Datenschutz kein Problem bei der EGK zu sein, nicht nur der Bundesbeauftragte Peter Schaar hat in Sachen Datenschutz keine Bedenken, auch Thilo Weichert, der oft kritische Schleswig-Hosteinische Datenschutzbeauftragte, gibt grünes Licht.

Die Projektträger erfüllten alle Auflagen der Datenschutzbeauftragten ohne langes Fackeln, da es bislang kein anderweitiges Interesse an der EGK gibt, das mit dem Datenschutz schwierig vereinbart werden muss. Die gesetzlich vorgesehenen Anwendungen, elektronische Gesundheitsakte, elektronisches Rezept, elektronischer Arztbrief, sind zur Zeit nicht mehr geplant. Außer Datenschutz kann die EGK noch nicht viel. Sie und ihre Telematik-Infrastruktur sind bislang weitgehend Selbstzweck. Hätte die IT-Industrie nicht Politiker und Funktionäre erfolgreich beeinflusst, wäre das Thema erledigt. Das Projekt könnte auch sterben, wenn eine dieser zentralen Anwendungen gleich live geht, weil dann erhebliche Probleme auftauchen. Das haben alle Pilotprojekte gezeigt: Endlose Wartezeiten vor den Terminals, von Arzt und Patient vergessene PINs, gesperrte Karten, Systemausfälle. Die Gematik macht es in ihrem Sinne richtig, die Karte beinahe ohne Anwendungen einzuführen. Uns ist niemand bekannt, der sich unbezahlt für die EGK eingesetzt hätte. Kein Arzt, kein Patient. Außer vertrieblich und infrastrukturell interessiert das Ding niemanden. Die EGK ist für den beamteten Datenschutz genauso eine 100 % Erfolgsstory, wie für die Hersteller von Chipkarten und Lesegeräten. Dass die Spezifikation der EGK von der Gematik gerade um Jahre zurück gekippt wurde, von 2.3.4 auf 0.5.3, ist für niemanden ein Problem, am wenigsten für die Gematik; sie darf weiter machen und bekommt Geld dafür. It‘s the economy, stupid.

Mit der EGK wird noch lange nur das gemacht werden, was schon mit der KVK ging. Den Stammdatenabgleich macht man schon viele Jahre gegen eine CD ROM, die monatlich an die Arztpraxen verteilt wird, Notfallausweise aus Papier haben Epileptiker und Diabetiker dabei. Die behalten sie auch, weil nicht jeder Arzt immer mit Lesegerät herumläuft. Organspendeausweise gibt es auch schon: menschenlesbar. Die Kosten der EGK-Infrastruktur bis jetzt: mehr als eine

Milliarde Euro, die von der Krankenversicherung an wenige Firmen überwiesen wurden, noch bevor die Infrastruktur im Wirkbetrieb ist. Warum soll man als ITler dagegen sein, das fragen sich selbst kritische Experten, und untersuchten den Aspekt Wirtschaftsförderung bisher nicht weiter. Das Ding schafft durchaus kurzfristig IT-Umsatz und Nachfrage nach Entwicklern, führt aber strategisch in eine Sackgasse.

Einige Hinweise für investigative Journalisten oder empörte Ärztinnen und Krankenpfleger, die keine Zeit mehr für Patienten haben, weil das Geld für die EGK bei ihnen eingespart wurde. Die folgenden Fakten sind bereits ausreichende Erklärung, warum es die EGK gibt.

Anke Martiny, Bundesvorsitzende von Transparency International, hat in mehreren Publikationen analysiert, wie die undurchsichtigen Lobbystrukturen im deutschen Gesundheitssystem Betrug und Korruption fördern.

Die großen Kassen, Barmer, DAK und TK, werden von ihren IT-Abteilungen dominiert, und die stehen seit den 1970er Jahren fest auf dem Boden der mentalen Welt von IBM-Großrechnern, großen Datenbanken, Prozessorientierung, big is beautiful.

Zwischen den Krankenkassen, mit ihren IT-Töchtern und Verbänden, und dem Bundesministerium für Gesundheit findet rege Personalunion statt. In Gesundheitsministerium und Kanzleramt sind ständig ausgeliehene Mitarbeiter des Krankenkassensystems im Einsatz.

Der Plan zur EGK wurde 2003 entwickelt, im Auftrag des Gesundheitsministeriums, vom Konsortium „bit4health“, ihm gehörten genau die Firmen an, die heute vom Projekt profitieren: Sagem Orga, IBM, Siemens, Giesecke & Devrient, IntercomponentWare.

Der wichtigste Profiteur der EGK in Deutschland ist Giesecke & Devrient GmbH, München. Laut Spiegel Nr. 11/2010 („Westerwelles Netzwerk“) gehört ihr Chef, Dr. Karsten Ottenberg, zum engsten geschäftlichen Netzwerk von Guido Westerwelle, dessen Mitglieder Westerwelle nicht verhungern lässt und die er zu Auslandsreisen mitnimmt. Dr. Karsten Ottenberg ist der Vorsitzende der Arbeitsgruppe 7, IKT und Gesundheit, des „Nationalen IT-Gipfels der Bundeskanzlerin“, der dem Land die strategische Richtung für die Entwicklung der staatlichen IT weist. Zu den Themen des IT-Gipfels gehören auch EGK und Gesundheits-Telematik.

Der Personalausweis als RFID-Chipkarte wird seit 2010 verteilt und ermöglicht eine rechtswirksame Identifikation und freiwillige Signatur mit PIN; damit ist eine maschinenlesbare Identifikation und Signatur für weitere Anwendungen zulässig. Er wird hergestellt mit wesentlicher Beteiligung von Giesecke & Devrient. Allerdings, für Giesecke & Devrient fällt bei einer Personalausweis-Anwendung wenig ab, aber dafür Millionen bei einer weiteren Chipkarte.

Für die CDU ist Deutschland Chipkartenland. 1999 wurde an Sagem Orga der Auftrag erteilt, eine Machbarkeitsstudie zur Asylcard zu erstellen. Bei der Bundeswehr wird derzeit der neue Elektronische Dienstausweis ausgegeben, eine Chipkarte, geplant seit 2001. Eine Chipkarte, die alle Arbeitslosen hätten kaufen müssen, („Job-Card“) war Bestandteil des jüngst gestoppten ELENA-Projekts. Ministerin von der Leyen fordert die Bildungs-Chipkarte für arme Kinder. Die Liste ist unvollständig.

Gesundheits-Chipkarten gibt es nur in den 2 Ländern, in denen weltweit führende Chipkartenhersteller sitzen (Deutschland und Frankreich), oder in welchen, die in Staatskorruptions-Indices von EU und Transparency International schlechte Plätze haben (Österreich, Slowenien, Taiwan), sonst nirgends.

Die gesetzliche Krankenversicherung zahlt vieles, was einige blöd finden. Valium, Homöopathie, Fluoxetin, Kneipp-Kuren und anderes. Warum nicht auch elektronische Gesundheitsakten und Rezepte. Solange sie genauso freiwillig sind. Sind sie das?

3. Die EGK als Thema für die occupy-Bewegung – oder: Datenschutz als Stellvertreterkrieg

„Ein kluger Fürst darf sein Versprechen nie halten, wenn es ihm schädlich ist oder die Umstände, unter denen er es gegeben hat, sich geändert haben“ (Niccoló Macchiavelli).

Die beiden wichtigsten Datenschützer, die gegen die EGK aktiv sind, heißen Wolfgang Linder und Kai-Uwe Steffens. Sie warnen nicht in erster Linie vor jetzt ausgerollten EGK-Anwendungen, sondern vor geplanten. Kai-Uwe Steffens verweist darauf, dass zentral gespeicherte Gesundheitsdaten und ihr Austausch über das Internet immer unsicher sind, die ganze Chipkarten-Infrastruktur aber nur Sinn hat, wenn es sie gibt. Wolfgang Linder vom „Komitee für Grundrechte und Demokratie“ warnt, für die Finanziers, die Krankenkassen, lohne sich die Infrastruktur erst, wenn neue Anwendungen kämen; sie sind in der Pipeline, die seien erst das Problem. (Siehe http://www.grundrechtekomitee.de/node/480 und das gerade erschienene Buch des Komitees für Grundrechte und Demokratie „Digitalisierte Patienten – Verkaufte Krankheiten“). Linder verweist auf Folgendes: Jede bisherige Regierung hat ins Gesetz geschrieben, was der Krankenkassenverband ihr diktiert, am genauesten CDU/FDP, deren Abgeordnete oft keine Ahnung haben, welchen Last-Minute-Gesetzen sie gerade zustimmen. Wenn die Opposition Einwände gegen ihr Gesetzprojekt vorbringt, rufen sie empört dazwischen „Zur Sache!“, weil sie annehmen, im Gesetzentwurf stehe nur, was ihr Minister gesagt hat. Volksvertreter haben oft keine Ahnung.

Im gleichen Blitzverfahren wird, laut Wolfgang Linder, eines Tages entweder die Freiwilligkeit bei der Elektronischen Patientenakte ausgehebelt, oder die Vorschrift, dass keiner benachteiligt werden darf, der diese Akte nicht haben will. Eins von beiden muss fallen, sonst haben all die Investitionen für die Krankenkassen keinen Sinn. Da wird er recht haben. Es geht den Kassen um Wettbewerb in der Krankenversorgung, um zu akzeptablen Kosten die älter und kränker werdende Bevölkerung zu versorgen. Hier kommt die occupy-Bewegung ins Spiel, denn es geht gleichzeitig um die ambulante Patientenversorgung als Investitionssphäre für Banken, Versicherungen und Klinikkonzerne. Viele Krankenkassen sind längst eng verbunden mit Privatversicherungen. Sie wollen mitbehandeln und Geld von der Ärzteschaft zu sich selbst umverteilen. Der Datenschutz erschwert dieses

„Managed Care", die EGK soll sie möglich machen.

Die Zukunft der Gesundheitsversorgung soll nämlich die „populationsorientierte integrierte Versorgung" sein. das steht schon im Gesetz: §§ 140 a bis d SGB V. Es geht um alle Versicherten ganzer PLZ-Regionen, oder um Großgruppen, wie alle Dialyse-Patienten eines Bundeslandes. Ihre Versorgung soll komplett von einem Klinikkonzern oder einer Health-Management-Gesellschaft übernommen werden. Die bekommt von einer Krankenkasse, oder von einem Verband von Kassen den Auftrag dazu. Den Auftrag bekommt, wer verspricht, es billiger zu machen als jetzt, billiger als andere. Der Klinikkonzern oder die Managementgesellschaft, die den Versorgungs-Zuschlag hat, darf sich Ärzte und Krankenhäuser aussuchen, zu denen man als Patient gehen darf. Sie vereinbaren mit diesen Ärzten die Bedingungen, können sie gegeneinander ausspielen („Selektivverträge"). Das geht, weil die freie Arztwahl der Patienten dabei eingeschränkt ist.

Es gibt im Gesundheitswesen keinen vernünftigen Menschen, der gegen Integrierte Versorgung ist - gegen das enge Verzahnen der verschiedenen Dienstleister bei der Behandlung. Allerdings ist diejenige Integrierte Versorgung, die derzeit in Deutschland geplante ist, eine von „oben" gesteuerte, kontrolliert von sog. Health Management Organizations (HMO) und Klinikkonzernen, nach US-Vorbild.

Für diese „integrierte Versorgung" ist die EGK in doppelter Weise zentraler Baustein. Zum einen liefert sie die Information, zu welcher Versorgungsgruppe ich als Patient gehöre. Wem ich sozusagen gehöre, wo ich behandelt werden darf, oder welche Zusatzversicherung ich habe. Dazu dient das Versicherten-Stammdaten-Management, die erste und wichtigste Funktion der EGK. Jede Arztpraxis kann sofort sehen, in welchem Programm ich bin, z.B. „Diabetiker", ob sie mich überhaupt behandeln darf, wie sie mich behandeln kann und muss. Zum anderen sind die gewünschten Kosten-Einsparungen nur möglich, wenn viele Seiten auf dieselben Behandlungsinformationen zugreifen. Klinikkonzerne und Health-Management-Gesellschaften wollen ihre ambulante Behandlung mit Leitlinien steuern und auf ihrer Grundlage verbindlich qualitätssichern („Managed Care"). So können sie ihre Kostenziele erreichen und Verluste vermeiden. Ärzte werden teilweise ersetzt durch Telemetrie-Anwendungen (z.B. bei Herzproblemen) oder durch medizinische Callcenter (bei Bagatellerkrankungen). Das funktioniert nur, wenn der Betreiber umfassenden Zugriff auf die Behandlungsdaten hat. Es muss für Managed Care übergreifende elektronische Gesundheits- oder Fallakten geben, im Besitz der Betreiber, mit Zugriffsmöglichkeit durch viele Behandler und case manager. Jetzt wissen Leserinnen und Leser, warum Krankenkassen und Ärzteverbände gerade so viele IT-Stellenanzeigen schalten. Mit dem Arztgeheimnis, das die Ärzte voneinander abschottet, könnten Patienten die Begrenzung ihrer Ansprüche aushebeln. In den Managed-Care-Projekten, die es bisher gab („Hausarztverträge") mussten die Patienten denn auch weitgehend auf ihr Patientengeheimnis verzichten. Was zu erheblichem Ärger mit den Datenschutzbeauftragten Thilo Weichert führte.

Ein Mitarbeiter der Techniker Krankenkasse schreibt: „Die integrierte Versorgung ergänzt im Wesentlichen die Regelversorgung, wird aber zukünftig Teile der Regelversorgung ersetzen. Ihr Anteil wird steigen, und durch technische Vernetzungen wie die Patientenakte werden Kooperation und Arbeitsteilung einen höheren Stellenwert bekommen." In der Szene der Krankenkassen und Ärzteverbände finden zu dem Themenkreis mehrfach jährlich Tagungen und Kongresse statt, es herrscht Goldgräberstimmung. Es geht um so viele Milliarden, dass die Kosten der EGK beinahe verhältnismäßig sind, wenn man Managed Care für sinnvoll hält. In den USA kennt man diese Health Management Organziations, wie Kaiser Permanente, schon lange. Manche versuchen sie gerade wieder loszuwerden. Weil Patienten dort jetzt wissen, wie recht Ehrlichmann hatte, der gesundheitspolitische Berater von Präsident Nixon. Der warnte vor 40 Jahren: „The less care they give, the more money they make" (http://www.kaiserthrive.org/kaiser-permanente-history/).

Klinikkonzerne und Krankenkassen drängen in die ambulante Versorgung. Das ist hier nur durchsetzbar mit dem Segen des Datenschutzes. Den Datenschutzsegen erhält Managed Care mit der EGK. Jede Krankenkasse, die Geld machen will, denkt, sie braucht deshalb die EGK. Jeder rationale ambulante Arzt, der um sein Einkommen fürchtet, dem alles andere egal ist, will die EGK verhindern, um Managed Care zu verhindern. Wir haben es mit einem datenschutzpolitischen Stellvertreterkrieg zu tun.

Ein etwas anderer medizinischer Datenaustausch, freiwillig, ohne Patente, basierend auf offenen Standards, wird international erfolgreich sein. Nach Lage der Dinge wird er nicht aus Deutschland kommen, wegen der Blockade-Konstellation: Krankenversicherungen – Datenschützer – Chipkartenindustrie.

4. Ist das noch Datenschutz?

„Es gibt Gesichter, die jedes Mal, wenn sie auftauchen, wieder etwas Neues mitbringen, etwas, das man bis dahin noch nicht an ihnen bemerkt hat, auch wenn man ihnen hundertmal begegnet ist" (Dostojewskij).

Sie wollen auch weiterhin ein unbeschriebenes Blatt sein, normalerweise. Das sind Sie nicht mehr, wenn ich Ihr Arzt bin und in Ihrer zentralen Gesundheitsakte keine Eintragungen sind, im Alter 40 oder 50. Es ist unwahrscheinlich, dass da nichts steht, weil Sie im Leben nie beim Arzt waren. Wahrscheinlicher ist, dass Sie mir etwas vorenthalten. Das denke ich, weil ich Ihre leere Akte sehe. Das denke ich auch, wenn Sie mir sagen: ich gebe Ihnen keinen Zugriff. Ich sehe Sie als neuen Patienten dann anders als jetzt. Bei allem, was Sie sagen, denke ich wegen dieser leeren Akte: „... und was noch? Was verschweigt er mir?"

Wenn Sie alles aufzeichnen lassen und dem Arzt alles zeigen, steht da vielleicht etwas, was Sie für zweifelhaft halten. So dass Sie nicht möchten, dass Ihr neuer Arzt anders auf diese Idee kommt, als von selbst. Das geht aber nicht mehr, hat er einmal gelesen, was der Kollege über Sie schrieb. Eine unbefangene Begegnung ist nicht mehr möglich, sobald die zentrale elektronische Gesundheitsakte existiert.

Wenn Sie möchten, dass Ihr Arzt nur weiß, was Sie sagen und was er feststellt, und dass er sich auf der Grundlage sein Urteil bildet, wenn Sie an diesem unbefangenen Urteil interessiert sind und an keinem andern, müssen Sie sich privat behandeln lassen. Dieses Urteil können Sie nicht mehr bekommen, wenn es einen definierten Ort gibt, an dem Metadaten über Ihre medizinische Akte stehen, auf die Ihr Arzt regelmäßig zugreifen soll. Bei Managed Care ist es nicht mal möglich, von einem zweiten Arzt eine zweite, unbefangene Meinung einzuholen, und alleine zu entscheiden, was man glauben will.

Wenn man davon ausgeht, dass das Verhältnis Arzt-Patient ein sehr enges Vertrauensverhältnis sein sollte, ist eine elektronische Patientenakte mit definiertem Ort ihrer Metadaten (z.B. Zugriffsrechte) genauso problematisch wie eine Beicht-Akte oder eine Sex-Akte. Sie verhindern unbefangene, unvorbelastete Begegnungen. Man kann machen, was man will, ist abgestempelt, sobald es den Ort für Metadaten gibt: als Geheimniskrämer, Informationsblockierer, als längst Kranker, als Mitmacher oder Verweigerer.

Vertrauen verschwindet aus der Gesellschaft, Misstrauen und Vorsicht nehmen überhand. Die Philosophin Michele Marzano hat ein Buch darüber geschrieben: „Le contrat de défiance". In den USA ist für Ärzte der Zeitaufwand für Dokumentation längst größer, als der für Patientenkontakt. Dahin geht der Trend auch hier. Die EGK ist Teil davon. Das Recht auf die Möglichkeit des Vertrauens schwindet. Auch im Gesundheitsbereich. Dazu gehört das Recht, seine Vergangenheit aus dem Augenblick heraus zu interpretieren, und vom anderen genau so wahrgenommen zu werden. Mehr Wettbewerb im Gesundheitswesen kann anders gehen. Auch Selektivverträge sind ohne personenbezogene Datensammlungen möglich.

Freiwillig ist eine Anwendung, bei der kein Mensch von Amts wegen gefragt wird, ob er sie nutzen will. Die außer jenen, die sich freiwillig eingetragen haben, niemanden kennt. Es gibt im Internet diverse Anwendungen für Gesundheitsdaten, mit unterschiedlicher Schutzintensität. Die GKV könnte solche Anwendungen auch erstellen und nutzen, gern mehrere, auch eine davon mit Chipkarte. Kein Arzt sollte die Möglichkeit haben, festzustellen, ob es bislang keine, eine oder mehrere elektronische Gesundheitsakten über Sie gibt, verteilt oder lokal, wenn Sie dem Arzt alle Rechte geben, von denen er weiß, dass jeder sie hat. Dann stimmt es, dass Sie dem Arzt freiwillig den Zugriff auf Ihre Akte geben. Selbstverständlich spricht sehr viel für gemeinsame Akten von mehreren Behandlern. Wer es braucht, soll es unbedingt machen. Freiwillig. Das heißt: man kann so oder anders, ohne Vertrauensverlust.

5. Die Chance für Privatheit

Die Entwicklung des Datenschutzes zur Massenbewegung, auch Open Source und Wikipedia zeigen, dass eine neue Form des Gemeinschaftsbewußtseins am Werden ist. Seltsamerweise gerade unter als unsozial geltenden Informatikern. Sorgsamer Umgang mit dem Kulturerbe, so könnte man das auf den Punkt bringen, ist nötig. Macht euren Blödsinn überall, aber macht ihn nicht mit unseren Gemeinschaftsgütern, z.B. nicht mit dem Internet, nicht mit Etherpad, nicht mit der Wikipedia, nicht mit dem Regenwald der Philippinen. Dieses Beharren auf Ernsthaftigkeit beim Umgang mit gewissen Ressourcen ist eine Haltung, die am automatisierten Fortschritt orientierte Institutionen und ihre Vertreter nicht einnehmen können. Um als realistisch zu gelten, müssen sie ihren Leuten beweisen, dass nichts heilig ist, alles seinen Preis hat.

Diese Ernsthaftigkeit bringen einige davon ins Gesundheitswesen ein. Die Anwendungen, gegen die sie am meisten sind, zentrale medizinische Akte, elektronisches Rezept, sollen seit 20 Jahren eingeführt werden, sind heute fast außer Diskussion. Sie wiegen sich nicht in Sicherheit, sehen ökonomische Interessen und politische Sachzwänge am Werk.

Kein Bild einschicken ist schön und gut, sagen sie, diese Datenschützer in den Initiativen „Stoppt die e-card" und „Arbeitskreis Vorratsdatenspeicherung". Es sei aber schon entschieden, wer kein Bild einschickt, kriegt eine EGK ohne Bild, die funktioniert genauso. Man kann bei der Krankenkasse beantragen, weiterhin auch ohne EGK versorgt zu werden. Gegen die vorhersehbare Ablehnung kann man dann mit Widerspruch und Klage nach Karlsruhe gehen. Das machen einige. Bisher gibt es noch keine Gerichtsentscheidung. Man kann diesen Antrag jederzeit stellen, nachdem man die EGK erhalten hat. Zu gegebener Zeit könnten sie eine größere Massenklage starten.

Parallel gibt es die Idee, bei der Techniker Krankenkasse als Modellversuch einen Datenschutz-Tarif zu beantragen. Und wenn sie den nirgends kriegen, eine Datenschutz-Krankenkasse zu gründen. Elektronische Medien sollten für die Selbstverwaltung benutzt werden. Gläserne Verwaltung, statt gläserne Patienten, ist die Utopie dahinter.

Krankenkassen und Verbände sagen, nur mit Managed Care könnten immer krankere Versicherte zu konstanten Kosten versorgt werden. Zu Privatisierung und Leistungskürzung gäbe es keine Alternative. Der Status Quo sei nicht zu halten. Damit haben sie SPD und Grüne überzeugt. Behördlicher Datenschutz und Gerichte sind nicht berechtigt, gesundheitspolitische Alternativmodelle vorzuschlagen. Sie müssen den Krankenkassen ihre Sachzwänge zum Nennwert abnehmen. Die sagen zum Beispiel, die EGK-Infrastruktur sei besser als Microsoft Health Vault (siehe http://www.microsoft.com/en-us/microsofthealth/products/microsoft-healthvault.aspx). Und das sei die einzige denkbare Alternative. Deswegen wäre die EGK Datenschutz!

Den Beweis für das Gegenteil – Vereinbarkeit von Patientengeheimnis, guter Versorgung, vertretbaren Kosten – steht noch aus. Es wird zunächst eine kleine Minderheit sein, die zeigt, dass es anders geht. Transparente Selbstverwaltung, Datenschutz und offene Standards werden Kern einer politischen Alternative in vielen Bereichen sein – auch im Gesundheitswesen.



Karsten Neumann

Betriebliche Datenschutzbeauftragte auch nach der EU-Verordnung – Analyse und Korrekturvorschlag zu Artikel 35 EU-DSGVO-E

Der Vorschlag der EU-Kommission in dem Entwurf einer einheitlichen Datenschutzgrundverordnung EU-DSGVO-E für den öffentlichen und den nicht-öffentlichen Bereich in Europa[1] stößt auf teils unberechtigt heftige Kritik von Datenschützern aus Deutschland. Vor allem die Kritik an der Regelung zur Bestellungspflicht eines Datenschutzbeauftragten scheint angesichts der behaupteten Konsequenz, in Deutschland würden tausende Datenschutzbeauftragten ihren Job verlieren und nur noch 0,3% aller Unternehmen unterfielen dieser Bestellungspflicht, besonders gravierend. Allerdings trifft sie nicht zu und könnte schon mit einer kleinen Korrektur eines offensichtlich redaktionellen Versehens ad acta gelegt werden. Zu diskutieren wäre jedoch, ob damit bereits alle Fälle risikobehafteter Datenverarbeitungen umfasst sind.

Der Kommissionsvorschlag sieht in Art. 35 Absatz 1 lit. a die Pflicht zur Bestellung eines Datenschutzbeauftragten für alle öffentlichen Stellen – unabhängig von der Art der Datenverarbeitung oder der Anzahl der Mitarbeiter – vor. Schon das ist selbst für diejenigen deutschen Bundesländer ein großer Fortschritt, in denen es nach den Landesdatenschutzgesetzen noch keine Pflicht zur Bestellung von Datenschutzbeauftragten gibt. In Verbindung mit den sonstigen in der EU-DSGVO-E vorgesehenen Vorgaben zu Qualifikation und Rahmenbedingungen für dessen Tätigkeit sind aber auch ganz generell in der Bundes-, der Landes- und der Kommunalverwaltung nicht unerhebliche Fortschritte zu erwarten; selbst dort, wo auch bisher schon Datenschutzbeauftragte bestellt waren.

Die öffentliche Kritik der Datenschutzverbände richtet sich vor allem gegen Artikel 35 Absatz 1 lit. b EU-DSGVO-E, wonach der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter einen Datenschutzbeauftragten benennen muss, falls „die Bearbeitung durch ein Unternehmen erfolgt, das 250 oder mehr Mitarbeiter beschäftigt“. Hiernach entstünde tatsächlich die ungewöhnliche Konstellation, dass beispielsweise ein großes medizinisches Rechenzentrum mit 100 Mitarbeitern von der Bestellungspflicht entbunden würde, eine Werft mit 1500 Mitarbeitern hingegen, in der lediglich in der Personalabteilung personenbezogene Daten verarbeitet werden, nicht. Dieser Eindruck muss allerdings sofort korrigiert werden, sieht man sich die folgende Regelung genauer an.

Nach Art. 35 Absatz 1 lit. c soll der für die Verarbeitung Verantwortliche einen Datenschutzbeauftragten benennen, falls „die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke eine regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen.“

Redaktionelles Versehen?

Bereits der Versuch, Fälle zu identifizieren, in denen Verarbeitungsvorgänge „aufgrund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke“ eine regelmäßige „Beobachtung von betroffenen Personen erforderlich machen“ könnte, lässt den Interpreten stutzen. Sollte hier wirkliche eine Spezialregelung für Fälle gemeint sein, in denen Protokolldaten erzeugt werden, um Mitarbeiterverhalten zu überwachen? Aber für welche Art von Unternehmen stellt eine solche Datenverarbeitung eine „Kerntätigkeit“ dar? Eine polizeiliche oder geheimdienstliche Tätigkeit kann hier schon nicht gemeint sein, da diese allenfalls durch den ebenfalls vorliegenden Richtlinienvorschlag umfasst würde.

Da liegt es nahe, sich in der Begründung des Verordnungsvorschlages nach einem Hinweis auf die Regelungsabsicht umzuschauen. Dort stößt der Ratsuchende auf folgende Formulierung:

„Artikel 35 schreibt die Einsetzung eines Datenschutzbeauftragten für den öffentlichen Sektor sowie im privaten Sektor für Großunternehmen und in Fällen vor, in denen die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters aus Verarbeitungsvorgängen besteht, die einer regelmäßigen, systematischen Überwachung bedürfen. Gestützt ist diese Bestimmung auf Artikel 18 Absatz 2 der Richtlinie 95/46/EG, der den Mitgliedstaaten die Möglichkeit bietet, als Ersatz für die allgemeine Meldepflicht die Bestellung eines Datenschutzbeauftragten vorzusehen“ (KOM (2012) 11/4, Begründung, Erläuterung des Vorschlag im Einzelnen 3.4.4.4. Abschnitt 4 – Datenschutzbeauftragter; Hervorhebung durch den Autor). Hiermit wird deutlich, dass es sich bei der Einfügung des Tatbestandsmerkmals „von betroffenen Personen“ nur um ein redaktionelles Versehen handeln kann und die Formulierung richtigerweise lauten muss: „welche aufgrund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke eine regelmäßige und systematische Beobachtung erforderlich machen“.

Zu diesem Ergebnis käme auch eine genauere Betrachtung der Übersetzung, wenn man von der englischen Arbeitsfassung ausgeht. Dort heißt es in der Begründung „which require regular and systematic monitorig”, im Gesetzestext

dann jedoch „require systematic monitoring of data subjects". Hier hat sich also wohl ein systematischer Fehler dann auch in der Übersetzung durchgesetzt.

Auslegungsbedürftiger Regelungsvorschlag

Damit wäre die Gefahr eines „Generalangriffs auf das deutsche Datenschutzniveau" jedoch noch nicht gebannt. Es stellt sich weiterhin die Frage, welche Datenverarbeitungsvorgänge denn dann eine regelmäßige und systematische Beobachtung durch einen betrieblichen Datenschutzbeauftragten erforderlich machen sollen. Die Antwort hierauf findet sich ebenfalls bereits im Verordnungsentwurf.

Unstreitig dürfte sein, dass genehmigungspflichtige Verarbeitungen offensichtlich gemeint sein dürften. Nach Artikel 34 Absatz 1 sind Verarbeitungen durch die Aufsichtsbehörde zu genehmigen, wenn der für die Verarbeitung Verantwortliche „Vertragsklauseln nach Artikel 42 Absatz 2 Buchstabe d vereinbart oder keine geeigneten Garantien für die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation in einem rechtsverbindlichen Instrument nach Artikel 42 Absatz 5 vorsieht".

Gemäß Artikel 33 Absatz 1 hat die verantwortliche Stelle aber bereits eine Datenschutz-Folgenabschätzung in den Fällen vorzunehmen, in denen Verarbeitungsvorgänge **aufgrund ihres Wesens, ihres Umfangs oder ihrer Zwecke konkrete Risiken für die Rechte und Freiheiten betroffener Personen bergen**. Dort werden diese ausführlich weiter konkretisiert:

„Die in Absatz 1 genannten Risiken bestehen insbesondere bei folgenden Verarbeitungsvorgängen:

a) systematische und umfassende Auswertung persönlicher Aspekte einer natürlichen Person, beispielsweise zwecks Analyse ihrer wirtschaftlichen Lage, ihres Aufenthaltsorts, ihres Gesundheitszustands, ihrer persönlichen Vorlieben, ihrer Zuverlässigkeit oder ihres Verhaltens oder zwecks diesbezüglicher Voraussagen, …

b) Verarbeitung von Daten über das Sexualleben, den Gesundheitszustand, die Rasse oder die ethnische Herkunft oder für die Erbringung von Gesundheitsdiensten, für epidemiologische Studien oder für Erhebungen über Geisteskrankheiten oder ansteckende Krankheiten,…;

c) weiträumige Überwachung öffentlich zugänglicher Bereiche, insbesondere mittels Videoüberwachung;

d) Verarbeitung personenbezogener Daten aus umfangreichen Dateien, die Daten über Kinder, genetische Daten oder biometrische Daten enthalten;

e) sonstige Verarbeitungsvorgänge, bei denen gemäß Artikel 34 Absatz 2 Buchstabe b vorab die Aufsichtsbehörde zu Rate zu ziehen ist."

Mit der Bezugnahme auf Artikel 34 Absatz 2 lit. b werden alle Fälle umfasst, in denen „die Aufsichtsbehörde eine vorherige Zurateziehung bezüglich der in Absatz 4 genannten Verarbeitungsvorgänge, welche aufgrund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke konkrete Risiken für die Rechte und Freiheiten betroffener Personen bergen können, für erforderlich hält." Hier eröffnet Artikel 34 Absatz 4 neben den aus anderen Gründen kritikwürdigen Regelungsbefugnissen der Kommission darüber hinaus eine Auslegungsbefugnis für die Aufsichtsbehörden. „Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, die Gegenstand der vorherigen Zurateziehung nach Absatz 2 Buchstabe b sind, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt derartige Listen an den Europäischen Datenschutzausschuss."

So begrüßenswert die Möglichkeit für Aufsichtsbehörden ist, den Katalog in einem einfachen Verfahren um neue Gefährdungsklassen zu erweitern und zu konkretisieren, so könnte und sollte er vom Gesetzgeber noch weiter mit dem Ziel beraten werden, ob hiermit bereits alle Regelfälle besonders risikoreicher Datenverarbeitungen umfasst sind. So könnte die Aufnahme von Verfahren zur Überwachung des Arbeitsverhaltens ebenso hilfreich sein, wie die generelle Aufnahme von Datenverarbeitungsverfahren, die sich an Kinder richten. Es erschließt sich auch nicht, warum einerseits besondere Arten personenbezogener Daten definiert werden, diese dann aber nur bei „umfangreichen" Dateien der Kontrolle eines betrieblichen Datenschutzbeauftragten unterzogen werden sollen. Hier sollte der Grundrechtsschutz nicht an eine bestimmte Menge von Betroffenen geknüpft werden.

Eine solche Liste von überwachungsbedürftigen Verarbeitungsvorgängen würde damit nach der hier vertretenen Auffassung nicht nur das Erfordernis einer internen und externen Vorabkontrolle auslösen, sondern auch die Pflicht zur Bestellung eines Datenschutzbeauftragten als Mittel einer effektiven und qualifizierten, betrieblichen Selbstkontrolle. Diese Lösung wäre auch sachgerecht, fließen so doch qualitativ bestimmbare Gefährdungsaspekte in die Bestellungspflicht für einen Datenschutzbeauftragten ein.

Zur Klarstellung einer solchen Auslegung des Verordnungsvorschlages wäre es hilfreich, im Rahmen der anstehenden parlamentarischen Beratung den Text wie folgt zu fassen:

„Artikel 35 Benennung eines Datenschutzbeauftragten

1. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter benennen einen Datenschutzbeauftragten, falls

a) die Verarbeitung durch eine Behörde oder eine öffentliche Einrichtung erfolgt; oder

b) die Bearbeitung durch ein Unternehmen erfolgt, das 250 oder mehr Mitarbeiter beschäftigt, oder

c) die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke eine regelmäßige und systematische Beobachtung **insbesondere in den Fällen der Artikel 33 und 34** erforderlich machen."

1 Vorschlag für VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM (2012) 11/4

BigBrotherAwards – Die Preisträger 2012

Behörden und Verwaltung: Innenminister Sachsen

Der BigBrotherAward 2012 in der Kategorie Behörden und Verwaltung geht an den Sächsischen Staatsminister des Inneren, Herrn Markus Ulbig, für Funkzellenabfragen im Raum Dresden. Nachdem am 19. Februar 2011 in Dresden 20.000 Menschen gegen einen Nazi-Aufmarsch demonstriert hatten, forderten das Landeskriminalamt und die Polizei in Dresden die Telekommunikationsverbindungsdaten für 28 Funkzellen an, die Masse davon aus dem örtlichen Bereich des Versammlungsgeschehens. Bald tauchten die erhobenen Daten in Strafverfahren auf, für die man sicher keine Funkzellenabfrage genehmigt bekommen hätte. Der Preisträger verteidigt den ausgelösten Daten-Tsunami von über einer Millionen Datensätze zu inzwischen mehr als 55.000 identifizierten Anschlussinhaberinnen und -inhabern bis heute als rechtmäßig.

Kommunikation: die Cloud

Der BigBrotherAward in der Kategorie Kommunikation geht an die Cloud als Trend, Nutzerinnen und Nutzern die Kontrolle über ihre Daten zu entziehen. Wer Adressbücher und Fotos – und damit die Daten anderer Menschen – oder Archive, Vertriebsinfos und Firmeninterna unverschlüsselt in den undurchsichtigen Nebel der Cloud verlagert, handelt mindestens fahrlässig. Fast alle Cloud-Anbieter sind amerikanische Firmen – und die sind laut Foreign Intelligence Surveillance Act verpflichtet, US-Behörden Zugriff auf alle Daten in der Cloud zu geben, auch wenn sich die Rechnerparks auf europäischem Boden befinden. Das 2008 vom Bundesverfassungsgericht postulierte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme wird damit eklatant verletzt.

Politik: Bundesinnenminister Hans-Peter Friedrich

Der BigBrotherAward 2012 in der Kategorie „Politik“ geht an Bundesinnenminister Dr. Hans-Peter Friedrich (CSU) für die Einrichtung eines Cyber-Abwehrzentrums ohne Legitimation durch den Bundestag, für die Einrichtung eines Gemeinsamen Abwehrzentrums gegen Rechtsextremismus (GAR), ebenfalls am Parlament vorbei, sowie für den Plan, alsbald eine gemeinsame zentrale Verbunddatei „gewaltbezogener Rechtsextremismus“ zu errichten. Mit der geplanten Verbunddatei und den neuen Abwehrzentren werden Polizei, Geheimdienste und teilweise das Militär auf problematische Weise vernetzt und verzahnt – unter Missachtung des historisch begründeten Verfassungsgebotes, nach dem diese Sicherheitsbehörden strikt voneinander getrennt sein und getrennt arbeiten müssen.

Verbraucherschutz: Blizzard Entertainment

Der BigBrotherAward 2012 in der Kategorie „Verbraucherschutz“ geht an die Firma Blizzard Entertainment für diverse Datenschutzverletzungen bei ihren Online-Spielen (z.B. World of Warcraft). Aus der protokollierten Spieldauer, erhobenen Rechnerdaten, dem Abgleich von Freundeslisten und dem zum Teil öffentlich im Netz einsehbaren Spielerverhalten (z.B. wie hat jemand eine bestimmte Aufgabe gelöst) lassen sich Persönlichkeitsprofile und Charakterstudien erstellen. Für eine entsprechende Auswertung wurde bereits 2007 ein US-Patent eingetragen – auf einen wissenschaftlichen Mitarbeiter von Google. Stück für Stück werden die Methoden zur Datenklauberei in den endlosen Nutzungsbedingungen weiter ausgeweitet. Immerhin: Der Versuch, den Zwang zu öffentlichen realen Klarnamen einzuführen, wurde durch Spielerproteste verhindert – noch.

Technik: Gamma International

Den BigBrotherAward in der Kategorie Technik erhält die Gamma Group, in Deutschland vertreten durch die Gamma International in München, namentlich den Prokuristen Stephan Oelkers, für ihre Software „FinFisher“. Gamma wirbt damit, dass Sicherheitslücken in iTunes und Skype genutzt werden, um z.B. per gefälschten Updates Spionagesoftware auf andere Rechner einzuschleusen und über ihre Software FinSpy Mobile auch auf Blackberrys zugreifen zu können. Gamma-Software wird an Geheimdienste und staatliche Institutionen im In- und Ausland verkauft. Gefunden wurde sie zum Beispiel bei der Erstürmung der Kairoer Zentrale des ägyptischen Geheimdienstes durch Bürgerrechtler.

Arbeitswelt: Bofrost

Der BigBrotherAward 2012 in der Kategorie Arbeitswelt geht an die Firma Bofrost für die rechtswidrige Ausforschung von Daten auf einem Betriebsratscomputer. Bofrost hat die Dateiinformation eines dort gefundenen Schreibens verwendet, um einem Betriebsratsmitglied zu kündigen. Das Arbeitsgericht hat die Unzulässigkeit dieses Vorgehens bestätigt. Auf einem Computer eines anderen Betriebsrats wurde ohne Zustimmung des Betriebsrats die Fernbedienungssoftware Ultra VNC installiert und erst nach gerichtlichem Vergleich wurde zugesichert, dies in Zukunft zu unterlassen.

Wirtschaft: Brita GmbH

Der BigBrotherAward in der Kategorie Wirtschaft geht an Herrn Markus Hankammer, vertretungsberechtigter Geschäftsführer der Firma Brita GmbH, für ihre kostenpflichtigen Wasserspender in Schulen, die unter dem Namen „Schoolwater“ vermarktet werden. Diese Geräte geben nur dann Wasser ab, wenn ein Kind es mit einer mit einem RFID-Funkchip verwanzten Flasche abzapft. Auf die Gefahren von Funkchips, die man berührungslos auslesen kann, ohne dass der/die Träger/in das bemerkt, haben wir in den vergangenen Jahren wiederholt hingewiesen. Dieses Wasserflaschen-System zeigt in besonders eklatanter Weise den Versuch, Übertechnisierung, Überwachung und Bevormundung schon im frühen Kindesalter zu etablieren. Außerdem kritisieren wir mit unserer Preisvergabe, dass damit

Leitungswasser zu einem teuren, exklusiven Lebensmittel gemacht wird, anstatt es Kindern in der Schule als allgemeine Gesundheitsvorsorge unbegrenzt zur Verfügung zu stellen.

Lobende Erwähnungen

Dr. Thilo Weichert, Datenschutzbeauftragter des Landes Schleswig-Holstein

Es gibt keine Positiv-Preise bei den BigBrotherAwards, aber dieses Jahr gibt zum ersten Mal „Lobende Erwähnungen". Und eine davon geht an Thilo Weichert. Gründe dafür gäbe es viele – kaum ein anderes Bundesland hat so ein engagiertes Datenschutzzentrum.

Die Datenschutzprobleme bei Facebook sind hinlänglich bekannt, auch wenn immer wieder neue ans Licht kommen. Insbesondere die Unmöglichkeit, Fanseiten datenschutzkonform zu betreiben und die Einbindung von „Like"-Buttons auf anderen Webseiten sind mittlerweile ein allgegenwärtiges Problem. Thilo Weichert hat es 2011 nicht mehr bei Warnungen an die Nutzer/innen belassen, sondern hat das Problem aktiv angegangen. Er hat öffentliche Stellen in Schleswig-Holstein, die Facebook-Fanseiten betreiben, verwarnt.

Facebook hat nominell keinen Firmensitz in Deutschland und macht es damit schwer, sie für Gesetzesverstöße zur Verantwortung zu ziehen. Die Aktion des ULD hält sich an diejenigen in Deutschland, die von Facebook profitieren. Und packt damit Facebook dort, wo es weh tut.

Billigen Spott und Häme gab es eine Menge, vor allem aus regierungsgeneigten IT-Kreisen. So hieß es schon in einer Eröffnungsrede des IT-Gipfels der Bundesregierung: „Das funktioniert in der ganzen Welt so – bis auf Schleswig-Holstein …" Interessant auch zu beobachten, wie schnell CDU-Parteigänger dann plötzlich die Maxime „legal, illegal, scheißegal" für sich entdecken.

Die Datenschutzbeauftragten des Bundes und der Länder haben Thilo Weichert per Erklärung des Düsseldorfer Kreises unterstützt, aber er bleibt neben Johannes Caspar aus Hamburg der Einzige, der sich traut, auch Taten folgen zu lassen.

Schließlich gibt es große Beachtung für sein Vorgehen gegen Facebook in der internationalen Presse – der Nachhall davon wird bei Facebook und auch anderen großen Datenkraken ohne Zweifel merkbar ankommen.

Intendant und Personalrat des Hessischen Rundfunks – HR

Das Elektronische Einkommens-Nachweissystem „Elena" wurde im Dezember 2011 nach massiven öffentlichen Protesten eingestellt. Im März 2010, knapp zwei Jahre davor, hatte der FoeBuD, der auch die BigBrotherAwards verleiht, eine Verfassungsbeschwerde im Namen von 22.000 beteiligten Bürgerinnen und Bürgern eingereicht. Ein Jahr später beteiligte sich der Hessische Rundfunk an diesem Protest in einer einzigartigen Aktion: Intendant, Personalrat und die beim Hessischen Rundfunk vertretenen Gewerkschaften haben im Frühjahr 2011 die Einstellung der Datenübermittlung angekündigt und die Bundesregierung aufgefordert, die Datensammlung zu beenden. HR-Intendant Helmut Reitze höchstpersönlich hat die Datenübermittlung gestoppt, obwohl das Gesetz zu diesem Zeitpunkt noch in Kraft war und er ein Bußgeldverfahren riskierte. Dies war ein Vorbild für andere Betriebe und Behörden. Konsequent und effektiv war auch die Informationsarbeit des HR-Personalrats Ulrich Breuer. Über seinen E-Mail-Verteiler hat er die interessierte Öffentlichkeit mit aktuellen Unterlagen und Hinweisen versorgt.

Tadelnde Erwähnungen

Principia GmbH & Co, KG, Düsseldorf

Mit der Installation von 16 Videokameras in einem Mietshaus wurden die Bewohner bespitzelt.

Hamburger „Gefährder-Ansprachen"

Bei 6.000 betroffenen Personen hat sich die Polizei in persönlichkeitsverletzender Weise Zutritt zu deren Wohnungen verschafft.

Lok8u

Die Firma Lok8u bietet ganz offen eine elektronische Armfessel für Kinder an, als Armbanduhr getarnt.

RWE

Die RWE Kundenservice GmbH, nötigt ihre Callcenter-Dienstleister, die Überwachungssoftware Click2Coach einzusetzen, mit der Aktivitäten der Callcentermitarbeiterinnen und –mitarbeiter aufgezeichnet werden.

Staatsanwaltschaft Köln

Die Behörde stellte im Frühjahr 2011 ein Telefonverzeichnis ins Internet, in dem die Zuständigkeit ihrer Abteilungen nach den Klarnamen von Beschuldigten sortiert war.

Diskos in Osnabrück

In Osnabrück haben die Betreiber von 18 Diskotheken vertraglich vereinbart, sich gegenseitig und der Polizei über eine schwarze Liste Namen von Menschen zu nennen, die bei ihnen Hausverbot bekommen.

Fusion-Festival – Kartenkontrollen

Bei der Open-Air-Veranstaltung „Fusion" in Mecklenburg-Vorpommern müssen Besucher zur Erlangung von Karten mit namentlicher Registrierung an einer Kartenlotterie teilnehmen.

WDR-Gigapixelfoto

Der WDR hat von der Veranstaltung „Rheinkultur" ein mehrere Gigapixel-großes Panorama der Besucher anfertigen lassen, das ein extremes Heranzoomen erlaubt. Per Facebook können Dritte, die einen ihrer Freunde auf dem Panorama erkannt haben, diesen per Pfeil-Markierung aus der anonymen Masse hervorheben.

GEZ

In Zukunft sollen die VermieterInnen gegenüber der GEZ Auskunft über ihre Mieter geben. Und bei Befreiung von den Rundfunkgebühren aus sozialen oder gesundheitlichen Gründen werden von der GEZ Kopien der entsprechenden Bescheide verlangt und komplett eingescannt.

Avaaz.org

Es ist problemlos möglich, herauszufinden, wer schon in dem großen avaaz-Verteiler drin ist. Ein nicht so bürgerbeteiligungsfreundlicher Staat könnte so schon mal flugs einen Abgleich mit seinen Dissidentenlisten machen.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

Das Ende der Geduld: Facebook nervt – nicht nur Schleswig-Holstein

Am 11. Mai 2012 ist Facebook erneut mit Vorschlägen für die Änderung seiner Datenverwendungsregeln an die Öffentlichkeit getreten. Zwei solcher Versuche des einseitigen Festlegens der Verarbeitungsbestimmungen waren schon erfolglos, weil jeweils über 7000 Nutzende den Vorschlägen widersprochen hatten. Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) hat die geplanten Änderungen gesichtet und musste feststellen, dass erneut keine wesentlichen Verbesserungen und sogar weitere Verschlechterungen aus Datenschutzsicht vorgesehen sind, z. B. Ermächtigungen für eine noch längere Speicherung und Nutzung der Daten. Wenn wirklich etwas mehr Transparenz hergestellt wird, dann dadurch, dass die unzulässigen Verarbeitungen genauer beschrieben werden.

Die vom irischen Datenschutzbeauftragten vor fünf Monaten geäußerte Kritik in einem Auditbericht wird zwar aufgegriffen, aber die dort geforderten tatsächlichen Änderungen nicht umgesetzt. Der Leiter des ULD, ´Thilo Weichert, kommentiert: „Facebook nervt, indem es die Öffentlichkeit mit immer wieder neuen Scheinmanövern hinhält. Facebook muss nicht einfach sein Kleingedrucktes ändern, sondern seine Geschäftspolitik und seine Datenverarbeitung. Hierüber muss dann Transparenz hergestellt werden. Reale Optionsmöglichkeiten sind für die Betroffenen einzurichten, wobei die Grundeinstellung auf weitestgehende Vertraulichkeit ausgerichtet sein muss. Die Übermittlung von Nutzungsdaten in die USA ist zu stoppen. Reale Transparenz könnte Facebook herstellen, indem das Unternehmen uns Aufsichtsbehörden aussagekräftige Dokumentationen vorlegen würde. Dies wurde dem ULD im September 2011 versprochen. Bis heute haben wir aber nichts erhalten.

Wir können Facebook-Nutzenden nur ein weiteres Mal empfehlen, gegen die geplanten Datenverwendungsrichtlinien Einspruch einzulegen. Forderungen dazu finden sich unter www.our-policy.org. Würden diese umgesetzt, wäre Facebook zwar noch nicht in der Rechtskonformität angelangt, aber auf dem Weg dorthin. Jedem, der meint, Facebook behördlich oder kommerziell nutzen zu müssen, empfehle ich die Lektüre der bisherigen und der geplanten Datenverwendungsregelungen, um zu erfahren, mit welchem windigen Unternehmen er kooperiert. Und wer meint, mit Datenschutzverstößen reich werden zu können und gefasst ist, sich hierbei zu täuschen, dem ist nach Börsengang von Facebook der Aktienkauf zu empfehlen. Das ULD hofft, dass das Verwaltungsgericht Schleswig jetzt bald die Termine für die Verfahren gegen unsere Facebook-Verfügungen festlegt, auch wenn zwei Kläger ihre Klagebegründungen immer noch nicht vorgelegt haben.“

Die geplanten Änderungen der Datenverwendungsrichtlinien finden sich unter https://www.facebook.com/note.php?note_id=10151730729670301

Wünsche zur Änderung können bis zum 18.05.2012 mit folgendem Text zum Ausdruck gebracht werden „Ich widerspreche den Änderungen und will über die Forderungen auf www.our-policy.org abstimmen“ unter https://www.facebook.com/note.php?note_id=10151730990165301

Eine Bewertung des Börsengangs von Thilo Weichert aus Datenschutzsicht ist zu finden unter http://theeuropean.de/thilo-weichert/11075-facebooks-umgang-mit-benutzerdaten.

Cartoon



Initiative Europe-v-Facebook

Facebooks große „Datenschutz-Abstimmung“: Nach 48 Stunden lag die Teilnahme bei 0,006288%

Wie berichtet hat Facebook diesen Freitag (1. Juni) eine Abstimmung über die vor 4 Wochen vorgeschlagenen Änderungen der Datenschutzrichtlinien online gestellt. Hintergrund ist, dass Facebook sich in seinen Geschäftsbedingungen selbst zu einer Abstimmung verpflichtet hat, wenn mehr als 7.000 Nutzer eine bestimmte Veränderung kommentieren. Die Aktion „our-policy.org“ hat über 40.000 Kommentare erreicht.

Wahlurne (sicherheitshalber) versteckt.

Anstatt nun, wie in den Bedingungen versprochen, den Nutzern die Wahl über die Änderungsvorschläge zu geben, führt Facebook einen absurden Eiertanz auf: Da die Wahl laut Facebook erst bindend sein soll, wenn 30% der Nutzer mitmachen, wurde sie so gut versteckt, dass es kein Nutzer mitbekommt. „Bis Sonntag um 18 Uhr haben nur 56.655 von 901 Mio. Nutzern abgestimmt, das sind 0,006288%“, so Max Schrems, Sprecher von europe-v-facebook.org. „Facebook betreibt hier wieder einmal offensichtliche Nutzerverarsche: Erst wird groß die Nutzerbeteiligung versprochen, dann wird zur Sicherheit die Wahlurne versteckt. Frei nach dem Motto: ‚Demokratie nur, wenn das Ergebnis sicher stimmt‘. Zuckerberg nahm anscheinend ‚Demokratieunterricht‘ in China.“

Pest oder Cholera.

In diesem Zusammenhang ist auch interessant, dass nicht etwa über die eingebrachten Änderungsvorschläge abgestimmt werden kann, sondern nur zwischen den alten und den neuen Datenschutzrichtlinien. „Das ist wie die Wahl zwischen Pest oder Cholera. Wir empfehlen derzeit trotzdem für die alten Bedingungen zu stimmen, da die neuen noch weniger Rechte für die Nutzer bringen.“ Bisher sind ca. 74% der Nutzer für die bestehenden Bedingungen.

Einfach an Gesetze halten.

Die nun vorgeschlagene neue Datenschutzrichtlinie würde viele Dinge noch verschlimmern und entspricht auch nicht den Auflagen der zuständigen irischen Datenschutzkommission. Dementsprechend hat sich auch die irische Behörde kritisch geäußert ebenso wie eine deutsche Datenschutzbehörde. Für europe-v-facebook.org ist daher klar: „Facebook soll endlich mit diesem endlosen Eiertanz aufhören und sich einfach an die Gesetze halten.“

Weitere Infos: Allgemeine Presseinfo zu „europe-v-facebook.org“

Erfolgreicher Widerstand gegen die Volkszählung

Zensus-Behörde verzichtet auf Zwangsgeldvollstreckung

8. Mai 2012

Aus Niedersachsen wird der erste Fall eines erfolgreichen Widerstands gegen die letztjährige Volkszählung („Zensus 2011“) gemeldet. Einem Verweigerer wurde nun amtlich mitgeteilt, dass seine Daten nicht mehr erforderlich seien, weil sie keinen Eingang in die Statistik mehr finden könnten. Die Zwangsgeldbescheide hätten damit „ihren Zweck verloren“.

Der von der so genannten 10-%-Haushalte-Stichprobe betroffene Bürger wurde seit Mai 2011 zur Auskunft persönlicher Daten über sich und sein Lebensumfeld gedrängt, zuletzt hatte man ihm sowohl mündlich als auch schriftlich sogar mit Zwangshaft gedroht.

Entsprechend unerwartet erhielt er folgenden Bescheid einer Erhebungsstelle aus Niedersachsen, der auch dem AK Zensus vorliegt. Darin heisst es wörtlich:

„Die Erhebungen auf Grundlage des ZensG 2011 sind inzwischen abgeschlossen. Damit hat die Zwangsgeldfestsetzung ihren Zweck verloren.“

Die Behörde vermeldet weiterhin, dass sie die Vollstreckung der Zwangsgelder einstellt, weist allerdings freundlich darauf hin, dass entstandene Verwaltungsgebühren dennoch zu entrichten seien. Diese betragen je nach Bundesland und Befragungsfall zwischen weniger als 30 Euro und bis zu über 100 Euro für jeden einzelnen Zwangsgeldbescheid.

Ob, in welchem Umfang und zu welcher Zeit landes- oder bundesweit mehr solcher Fälle bekannt werden, ist zwar unklar, allerdings zeigt dieser Bescheid, dass ein Ende der Datenerfassung in Sicht ist und laufende Verfahren praktisch gegenstandslos werden.

„Selbst wenn andere Erhebungsstellen noch ein wenig länger brauchen sollten, um ihre ‚Erhebungen‘ abzuschließen, so läutet diese Nachricht doch unzweifelhaft das Ende der Zwangsmaßnahmen für die Haushaltsbefragten ein,“ sagt Michael Ebeling vom Arbeitskreis Zensus. „Viele Menschen haben sich bei uns gemeldet und von ihren Nöten durch bürokratische und bedrückende Drohgebärden der Behörden berichtet. Es wäre gut, wenn diese unsere Gesellschaft beschämenden Handlungen nun endlich ein Ende finden.“

Weitere Infos: http://zensus11.de/

Gemeinsame Kampagne und Video gegen Vorratsdatenspeicherung – PM des CCC, AK Vorrat und FoeBuD (23.05.2012)

Zum Jahrestag des Inkrafttretens des Grundgesetzes am 23. Mai geht der Kampf gegen die Vorratsdatenspeicherung in die nächste Runde: Der Chaos Computer Club (CCC), der FoeBuD und der Arbeitskreis Vorratsdatenspeicherung wenden sich erneut gegen die Pläne von Innenminister Hans-Peter Friedrich, die umstrittene EU-Richtlinie in Deutschland umzusetzen. Wir fordern, dass sich der Petitionsausschuss des Bundestags endlich mit dem von tausenden Bürgern unterzeichneten Anliegen befasst.

Zum Auftakt der Kampagne „STOP-VDS.de" erläutert ein Kampagnenvideo die Gefahren und Maßlosigkeit der anlasslosen Massenüberwachung in Kurzform[1]. Jeder kann das Video im Internet weiterverbreiten. Auf der Webseite der Kampagne befinden sich Bilder und Webseiten-Banner, mit denen Unterstützer ihren Protest ausdrücken können: STOP-VDS.de

„Die Kampagne vermittelt das komplexe Thema Vorratsdatenspeicherung mit einfachen Bildern und erklärt den Stand der derzeitigen Diskussion in Deutschland und der EU", sagte Dirk Engling, Sprecher des Chaos Computer Clubs. „Es geht bei der Kampagne darum, den Menschen zu zeigen, warum es gefährlich ist, wenn anhand der alltäglichen Kommunikation detaillierte Freundschafts- und Bewegungsprofile erstellt werden", so Werner Hülsmann vom Arbeitskreis Vorratsdatenspeicherung. „Vorratsdatenspeicherung betrifft die Privatsphäre aller Bürgerinnen und Bürger."

„Die Speicherung sämtlicher Telefonverbindungen wird von weiten Teilen der Bevölkerung abgelehnt: insbesondere Ärzte, Juristen, Gewerkschaften und Bürgerrechtsorganisationen haben sich mehrfach gegen die anlasslose Protokollierung aller Verbindungsdaten ausgesprochen. Auch Ermittler der Polizei zweifeln den Nutzen der Vorratsdatenspeicherung mittlerweile an", so Rena Tangens vom FoeBuD [2, 3].

Mehr als 64.000 Bürgerinnen und Bürger haben eine Petition mitgezeichnet, die sich für ein Verbot der Vorratsdatenspeicherung ausspricht. „Wir warten noch immer auf einen Termin für die Anhörung vor dem Petitionsauschuss des Bundestags", rief Werner Hülsmann vom Arbeitskreis Vorratsdatenspeicherung in Erinnerung. „Es ist bedenklich, dass der Ausschuss sich fortwährend über das berechtigte Begehren aus der Bevölkerung zur Mitsprache hinwegsetzt."

„Seit Jahren spricht sich eine klare Mehrheit der Bevölkerung gegen die Vorratsdatenspeicherung aus", sagte Dirk Engling, Sprecher des CCC. „Die Unterzeichner der Petition sollten wie der Souverän behandelt werden, nicht wie lästige Bittsteller, deren Unmut man jahrelang aussitzen kann."

Verweise:

1 Initiative STOP-VDS: http://www.stop-vds.de

2 Gemeinsame Erklärung anlässlich des 6jährigen Bestehens der Richtline zur Vorratsdatenspeicherung: http://www.vorratsdatenspeicherung.de/content/view/515/188/lang,de/

3 Wissenschaftliches Gutachten belegt: keine „Schutzlücke" ohneVorratsdatenspeicherung: http://www.ccc.de/de/updates/2012/mythos-schutzluecke



BvD: Über 200 Datenschutzbeauftragte diskutierten neue Wege im Datenschutz

Teilnehmerrekord bei zweitägiger Veranstaltung in Berlin – Beim Aktionstag „Datenschutz geht zur Schule“ wurden über 500 Schüler sensibilisiert.



Berlin, 22. Mai 2012

Über neue Wege im Datenschutz tauschten sich über 200 interne und externe Datenschutzbeauftragte, Vertreter der Aufsichtsbehörden und Gäste auf den BvD Verbandstagen aus. Auf dem jährlich stattfindenden Treffen der im Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. organisierten Datenschutzbeauftragten setzten sich die Experten über Vorträge und Workshops mit der Zukunft des Datenschutzes auseinander – hier insbesondere mit den Auswirkungen der EU-Datenschutzverordnung.

Der Bundesdatenschutzbeauftragte für den Datenschutz und die Informationsfreiheit, Peter Schaar, eröffnete den BvD Verbandstag mit einem Vortrag zur EU-Datenschutzreform und lotete die Auswirkungen für den nationalen und internationalen Datenschutz aus. Eine Modernisierung des Datenschutzgesetzes und eine EU-weite Vereinheitlichung begrüßte Schaar, denn Datenschutz lasse sich allein national immer weniger durchsetzen. Mit Blick auf die Datenschutzbeauftragten in Betrieben bezeichnete er einzelne Ausführungen der EU-Verordnung als verbesserungswürdig. So befand Schaar beispielsweise die 250-Mitarbeiter-Grenze, ab der die Bestellung eines Datenschutzbeauftragten für Unternehmen verpflichtend sein soll, als „willkürlich und zu hochgegriffen“. Vielmehr müssen als Kriterium die Art und Sensibilität der zu verarbeitenden Daten für Unternehmen und insbesondere für Dienstleister stärker in den Vordergrund gestellt werden.

Dr. Stefan Brink, Leiter „Privater Datenschutz“ bei der Landesbehörde für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, wies im Anschluss in seinem Vortrag deutlich auf Schwächen des Entwurfs der EU-Kommission hin. Die Grundverordnung führe dazu, dass die Datenschutzgesetze von Bund und Ländern abgelöst würden und das Bundesverfassungsgericht als Kontrollinstanz beiseite geschoben werde. Eine EU-Harmonisierung senke die deutschen Standards, auch in Bezug auf die betrieblichen Datenschutzbeauftragten. Brink argumentierte für das Prinzip des Föderalismus und plädierte für eine Verteidigung des bestehenden Niveaus in Deutschland: „Datenschutz ist zu wichtig, um es anderen zu überlassen.“

In 13 fundierten Workshops wurden die Inhalte der Vorträge weiter vertieft. BvD-Mitglieder und Gäste des BvD diskutierten hier neueste Entwicklungen im Datenschutz und erhielten von renommierten Referenten Praxistipps und gesichertes Know-how. „Das professionelle Angebot der Workshops wurde intensiv genutzt, alle Workshops waren sehr gut besucht“, bilanzierte Thomas Spaeing, Vorstandsvorsitzender des BvD e.V. Ein Ausstellerbereich mit einem Angebot im Bereich des Datenschutzes rundete die Veranstaltung ab.

Bereits einen Tag zuvor stand das umfangreiche Sonderprogramm mit einem Seminarangebot, BvD-Arbeitskreissitzungen und der BvD-Mitgliederversammlung an. „Auch das Seminarangebot war ein voller Erfolg, es war schnell ausgebucht“, sagte Jürgen Hartz, stellvertretender Vorstandsvorsitzender und im BvD-Vorstand unter anderem zuständig für die Veranstaltungsorganisation. Bei den Arbeitskreissitzungen konnten interessierte Mitglieder Einblicke in die ehrenamtliche Verbandsarbeit bekommen.

Eine Besonderheit war die Aktion „Datenschutz geht zur Schule“, die in diesem Jahr Teil der BvD-Verbandstage war. Beim diesem Projekt sensibilisieren speziell ausgebildete Datenschutzbeauftragte Schülerinnen und Schüler im Umgang mit persönlichen Daten. Beim Aktionstag war ein gutes Dutzend Dozenten am Berliner John-Lennon-Gymnasium unterwegs. Über 500 Schüler wurden am Aktionstag sensibilisiert, insgesamt sind es bereits über 25.000 Schüler an mehr als 200 Schulen bundesweit. Edgar Wagner, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, war Schirmherr der Aktion in Berlin. Die Initiative „Datenschutz geht zur Schule“ ist zudem Preisträger im Wettbewerb „365 Orte im Land der Ideen“ und „Ausgewählter Ort 2011“.

Mit der großen Resonanz auf die BvD-Verbandstage war der BvD-Vorstand sehr zufrieden. „Die BvD Verbandstage haben sich zu einer festen Größe im Datenschutzkalender der Datenschutzbeauftragten entwickelt“, freute sich Thomas Spaeing. Dem werde man auch im kommenden Jahr mit einem attraktiven Programm Rechnung tragen. Die auf den Verbandstagen diskutierten Aspekte – gerade zur EU-Datenschutzverordnung – werde der BvD zusammentragen und entsprechend in Politik und Wirtschaft hineintragen, um das Berufsbild des Datenschutzbeauftragten mit seinen Aufgaben, Rechten und Pflichten weiter zu schärfen und für adäquate Rahmenbedingungen zur Berufsausübung zu sorgen. Wichtiger Termin in diesem Zusammenhang wird das Berufsbildsymposium des BvD e.V. am 25. und 26. Oktober 2012 in Düsseldorf sein.

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Facebook kaufte StudiVZ nicht wegen Datenschutz

Die Verkaufsverhandlungen zwischen Facebook und Holtzbrinck, dem Eigentümer des sozialen Netzwerks StudiVZ, vor einigen Jahren sind anscheinend am Datenschutz gescheitert. Diese seien sehr weit fortgeschritten gewesen, sagte Markus Schunk, Chef des StudiVZ-Eigentümers Holtzbrinck Digital. Letztendlich sei der Verkauf „an datenschutzrechtlichen Auflagen gescheitert, die wir gar nicht beeinflussen konnten“. Der Stuttgarter Holtzbrinck-Verlag hatte StudiVZ 2007 übernommen und gut 80 Millionen Euro für das heute strauchelnde Berliner Startup auf den Tisch gelegt. Ein Verkauf an Facebook wäre für den Konzern lukrativ gewesen: Facebook-Gründer Mark Zuckerberg habe Holtzbrinck eine Beteiligung an Facebook angeboten, die angesichts des Börsengangs des US-Unternehmens heute wohl Milliarden wert wäre. Facebook zählt inzwischen weltweit rund 900 Millionen Nutzende. Dem Netzwerk StudiVZ kehren hingegen immer mehr Nutzende den Rücken. Die Zahl der monatlichen Besuche schwand von in der Spitze 466 Millionen - das war im Mai 2010 - auf 77 Millionen Ende 2011, wie Zahlen der Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern e.V. (IVW) zeigen, die die Reichweiten von Medien misst (www.sueddeutsche.de 09.04.2012).

Bund

Kontrollwahn bei Aldi

Andreas Straub ist ein Jungmanager, der mit 22 Jahren bei Aldi Süd eingestellt wurde. Inzwischen ist er ausgestiegen und hat das Buch „Aldi – einfach billig. Ein ehemaliger Manager packt aus“, verfasst, das über eine Vielzahl fragwürdiger Praktiken bei den beiden Unternehmen Aldi Süd und Aldi Nord berichtet. Straub zeichnet das Bild zweier paranoider Konzerne, die ihren Hierarchie- und Kontrollwahn an vielen Stellen bis zum Exzess treiben, Mitarbeitende, die nicht ins Raster passen, mobbt, mürbe macht und schließlich rausschmeißt. Von Kontrolle und Überwachung könnten alle betroffen sein: VerkäuferInnen, Manager, Zulieferer und KundInnen. Er sowie in eigener Recherche der Spiegel berichten über Aufsichtsmaßnahmen über die mehr als 100.000 weltweit tätigen Mitarbeitenden und Zulieferer, die nicht nur gegen den guten Geschmack, sondern insbesondere auch Gesetze, insbesondere gegen Arbeitsrecht verstießen. Auch nach dem Überwachungsskandal beim Erzrivalen Lidl im Jahr 2008 habe Aldi v. a. KundInnen und Beschäftigte überwacht. Zwar sei man nach der Affäre zunächst nervös geworden und habe einige Kameras abgebaut. Nach Feststellungen von Aussteiger Straub wurden die Kameras aber nur kurzfristig verpönt und bald danach aufgerüstet, wie aus einem Vermerk hervorgeht: „Diese Umrüstarbeiten haben absolute Priorität und müssen umgehend erledigt werden“. In Einzelfällen einiger hessischer Filialen, etwa in Frankfurt am Main oder in Dieburg, seien sommerlich leicht gekleidete KundInnen auch mal gerne rangezoomt worden. Vor allem Frauen in kurzen Röcken oder mit ausgeschnittenen Tops wurden heimlich gefilmt, etwa wie sie sich über Kühltheken beugten oder vor Regalen bückten. Die Bilder seien auf CD gebrannt und im Kollegenkreis verteilt worden.

Grundlage für den Aldi-Führungsstil ist das sog. Harzburger Modell, eine Managementmethode, die Mitte des 20. Jahrhunderts von Reinhard Höhn entwickelt wurde und nach dem Grundsatz arbeitet, Verantwortung an Mitarbeitende zu delegieren, diese dabei aber streng zu kontrollieren. Kontrolliert werde alles, bis hin zur möglichen Verkalkung der Perlatoren an den Waschbecken der Umkleideräume oder bis zum Löschen des Lichtes beim Verlassen eines Raumes. Gibt es Beanstandungen, so könne dies leicht zu Abmahnungen führen. Detektive werden als Testkäufer losgeschickt, um hinterher KassierInnen z. B. eine Abmahnung wegen „unkonzentrierten Arbeitens“ oder Verstoßes „gegen die Pflichten Ihres Dienstvertrages und der Dienstanweisung für Kassiertätigkeit“ aussprechen zu können. Abmahnungen sollen nicht Ultima Ratio sein, sondern gehören zum Tagesgeschäft, für das es bei Aldi Süd extra Vordrucke („Abreißblock“) gibt, in denen nur noch Namen und Datum eingetragen werden müssen. Einem Filialleiter in der Regionalgesellschaft Altenstadt wurde durch Vorgesetzte Ware in den Spind zu legen versucht, um ihn des vermeintlichen Diebstahls zu überführen und damit einen Kündigungsgrund zu konstruieren. Das Ertragen der Kontrolle und der Leistungsdruck werden mit einer übertariflichen Entlohnung zu erzwingen versucht.

Bei der Videoüberwachung ist auch der Kassenbereich betroffen. Die Detektive des Unternehmens speichern die Bilder über Wochen auf Datenträgern, auch wenn sich bei der Auswertung keine Unregelmäßigkeiten ergeben haben. Von den Detektiven werden „in Verdachtsfällen“ außerdem mobile Miniaturkameras installiert. So heißt es in einem Rahmenvertrag zwar: „Der Ladendetektiv darf eigene Kameras zur Überwachung der Lebensmitteldiscounteinzelhandelsfilialen nicht einsetzen.“ Doch habe das Unternehmen, das diesen Vertrag

mit einem Detektiv schloss, bei ihm die Anschaffung einer solchen Anlage durchgeführt. Mobile Kameras kamen bei Aldi Süd nicht nur in den Verkaufsräumen zum Einsatz, sondern auch dort, wo es keinen Kundenkontakt gibt, etwa in den Zentrallagern, auch wenn hierauf nicht hingewiesen wird.

Zwischen 2009 und 2010 hat Aldi Süd nach eigenen Angaben mit einem unabhängigen Datenschutzbeauftragten und dem Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen ein neues Videoüberwachungskonzept entwickelt. Bei Kameras im Kassenbereich werde danach sichergestellt, dass „die PIN-Eingabe keinesfalls einsehbar wird“. Dem gegenüber gibt es Hinweise, dass Kameras eindeutig das EC-Karten-Terminal erfassen und die Bilder so stark herangezoomt werden können, dass jede einzelne Ziffer erkennbar ist. Gemäß Aldi Süd erfolgt die Datenspeicherung „nur zur Sicherung von Beweismaterial nach außergewöhnlichen Ereignissen (Straftaten, Unfälle, Brände oder ähnliches)“. Mobile Kameras würden nicht durch Detektive, sondern von eigens beauftragten Technikern installiert und nur zum „Schutz unserer Mitarbeiter, Kunden und Lieferanten bei Gefahrensituationen und Überfällen, zur Prävention und zum Schutz des Eigentums eingesetzt“. Fälle, in denen mobile Kameras zusätzlich zu den fest installierten Videoanlagen eingesetzt wurden, seien nicht bekannt. Aldi Nord setzt nach eigenen Angaben Kameras „gleich ob festinstallierte oder mobile – nur ausnahmsweise in einzelnen Märkten ein“, nämlich „wenn sehr hohe Diebstähle zu verzeichnen sind“. Das Filmen der Kassenbereiche und damit die Aufnahme der Eingabe von PIN-Nummern würden bei Aldi Nord „strikt ausgeschlossen“.

Als im Jahr 2009 geplante Preisveränderungen vorab an Lidl durchgestochen worden waren, wurden alle Bezirksleiter angewiesen, sämtliche Fax-Protokolle ihrer Filialen auf Nummern in Neckarsulm, wo die Lidl-Zentrale sitzt, zu überprüfen. Gebracht hat dies nichts (Amann, Tietz Der Spiegel 18/2012; www.spiegel.de 29.04.2012; Giesen SZ 30.04./01.05.2012, 17).

Bund

Shitstorm gegen Aktionsteilnehmende für ihr Urheberrecht

Die InitiatorInnen und UnterzeichnerInnen des Appells „Wir sind die Urheber“ wurden von GegnerInnen ihrer Aktion, die sich zum Kreis der weltweit operierenden Gruppe „Anonymous“ zählen, im Internet mit sensiblen Daten bloßzustellen versucht. Auf einer Filesharingseite, auf der zuletzt massenhaft Daten von Twitter-Nutzenden zu lesen waren, wurden Name, Adresse, Telefonnummer, Fax- und E-Mailadresse von den SchriftstellerInnen, Intellektuellen und KünstlerInnen veröffentlicht, die hinter dem Anfang Mai 2012 in der „Zeit“ und im Internet veröffentlichten Aufruf „wir-sind-die-urheber.de“ stekken, von A wie Abyün über Kehlmann, Roche und Walser bis hin zu Z wie Zischler. Insgesamt haben sich 6000 KünstlerInnen dem Appell angeschlossen, nicht alle Namen sind im Internet publiziert. Doch Anonymous hat viele der Unterzeichnenden mit Datensteckbriefen versehen, offensichtlich, um weitere Unterstützende davon abzuhalten, sich zu solidarisieren. Der Koordinator der Aktion Matthias Landwehr interpretierte: „Es geht hier um Bloßstellung und Bedrohung, wie man sie aus totalitären Staaten kennt.“ Das spreche einer demokratischen Diskussionskultur hohn. Selbstverständlich könne man anderer Meinung sein, „aber dass Künstler von sogenannten Freiheitshelden bedroht werden, ist eine neue Dimension“.

Auf der Webseite „Wir sind die Urheber“ wird darauf hingewiesen, dass die detaillierten persönlichen Angaben der Unterzeichner nicht bei der Initiative selbst erbeutet worden sein können. Diese Daten stammten teilweise aus nicht leicht zugänglichen Quellen; sie müssten durch gezielte Recherche und Aushorchung erlangt worden sein. So wird z. B. Günter Wallraff, der wegen seiner Arbeit besonderen Wert darauf legen muss, nicht von jedem Menschen identifizierbar zu sein, von der Anonymous-Gruppe als Zielperson aufgeführt. Auf der Prangerseite wird die Aktion erläutert: „Fuck your copyright blah blah blah“. Falls die Unterzeichnenden nicht von ihrem Vorhaben abließen, heißt es - in drohender Gossensprache - würden sie weiterhin verfolgt, verfolgt und verfolgt - und man werde weitere Daten offenlegen. Einen Geschmack davon bekamen die KrimischriftstellerInnen des etwas kleiner angelegten Aufrufs „Ja zum Urheberrecht“ mit, die eine Plakataktion Ende April 2012 gestartet hatten, wo dargestellt wird, wie AutorInnen von einem eine Guy-Fawkes-Maske tragenden Herrn umgebracht und buchstäblich ausgenommen werden. Die Webseite der sechs AutorInnen wurde mit einer Massenmailattacke lahmgelegt; die InitiatorInnen wurden mit Hass-Mails eingedeckt und persönlich bedroht. Allein bei Nina George gingen innerhalb von einer Stunde 100.000 Mails ein, was dazu führte, dass der Provider deren Netzzugang kappte. Es sollen von dieser Anonymous-Attacke auch völlig Unbeteiligte betroffen gewesen sein. Es ist offensichtlich das erste Mal, dass Anonymous explizit Privatpersonen angreift. Bisher waren es Firmen und Organisationen gewesen wie Visa, Mastercard oder die Gema.

Die Autorin George meinte: „Wir müssen zu einem Ausgleich der verschiedenen Interessen kommen.“ Aber diskutieren könne man nur „mit einem Gegenüber, das sein Gesicht zeigt und Verantwortung für seine Haltung übernimmt. Anonyme Repressalien gegen Andersdenkende auszuüben ist feige und verachtenswert“. Wer „feige aus dem digitalen Dunkel heraus virtuelle Steine wirft“, den wolle sie nicht ernst nehmen. Doch sei es wohl ein Phänomen der Zeit, dass manche im Internet auf „Diskriminierung und kleingeistige, selbstverliebte Selbstjustiz“ setzten. Inzwischen wundere ich mich nur noch: Ich finde es erstaunlich, dass eine Gruppe, die sich totale Transparenz und völlige Freiheit aller Informationen auf die Fahne geschrieben hat, am liebsten im Schatten der Anonymität agiert. Die Ironie dieser Geschichte ist, dass wir uns nun ausgerechnet bei Facebook am sichersten fühlen, unter dem Dach eines Konzerns, von dem jeder weiß, dass er die Daten seiner Nutzer sammelt.“ Doch dürfe man, so die Autorin Angela Eßer, nicht schwei-

gen, denn dann hätten die Anonymous-Aktivisten ja ihr Ziel erreicht. In den Foren von Anonymous hieß es derweil „Tango down“ als Triumphnachricht, dass das ausgemachte Ziel getroffen wurde. Durch die Verbreitung über Twitter durch Anonymous z. B. gegen die Plakataktion am 26.04.2012 wurde die Aktion innerhalb kürzester Zeit erst richtig verbreitet und intensiv diskutiert. Tatsächlich führte der Anonymous-Angriff auch dazu, dass die Urheberrechtskampagene in einer breiteren Öffentlichkeit wahrgenommen wurde (Hanfeld, FAZ 14.05.2012, 27; Rapp, Der Spiegel 20/2012, 140 f.).

Bundesweit

„Aus“ für Schultrojaner

Nach massiven Kritiken an den Schulen und kritischen Berichten in den Medien haben die Verlage den Schultrojaner aufgegeben. Das bayerische Kultusministerium gab bekannt: „Eine Scansoftware für Schulen wird nicht kommen. Das ist das Ergebnis der Verhandlungen, die eine bayerische Delegation für die deutschen Länder mit den Schulbuchverlagen geführt hat.“ Die Kultusministerkonferenz (KMK) hatte 2010 mit den Schulbuchverlagen und Verwertungsgesellschaften einen Vertrag geschlossen, nach dem eine Spähsoftware in Schulnetzwerken nach unerlaubten Kopien suchen kann. Bundesjustizministerin Sabine Leutheusser-Schnarrenberger (FDP) hatte die Vereinbarung zwischen der KMK und den Schulbuchverlagen aus Datenschutzgründen scharf kritisiert. Das Recht der Urheber und Verlage an ihrem geistigen Eigentum sei ein hohes Gut, das an den Schulen respektiert und geschützt werde, sagte der Chef des bayerischen Kultusministeriums Peter Müller. Es komme aber darauf an, zu Lösungen zu kommen, die der „Bildungs- und Lebenswirklichkeit im 21. Jahrhundert“ entsprechen. „Unsere Partner in den Verhandlungen haben Augenmaß und einen hohen Grad an Verständigungswillen im Interesse der Schulen bewiesen.“ Der Einsatz der Software war für das Frühjahr 2012 geplant.

Die Plagiatssoftware zur Überprüfung von Speichersystemen der Schulen werde nicht eingesetzt. Auch Schulbestätigungen und Verpflichtungserklärungen, dass sich keine digitalisierten Unterrichtswerke auf Schulrechnern befinden, würden nicht mehr eingefordert. Die Schulbuchverlage sollten Möglichkeiten zur digitalen Nutzung von Unterrichtswerken und -materialien anbieten. Noch im Sommer würden Gespräche aufgenommen, um Lösungen zu erarbeiten. Der Vorsitzende des Deutschen Philologenverbandes, Heinz-Peter Meidinger, führte das Einlenken auf die vehementen Proteste an den Schulen, die Kritik von Datenschützern und des Bundesjustizministeriums zurück: „Es ist wohl jedem der Beteiligten bewusst geworden, dass die Entwicklung und der Einsatz einer solchen Software, die den datenschutzrechtlichen Anforderungen genügt, nicht möglich ist. Wichtiger fast noch als die Einräumung von Rechten zu analogen Kopien ist für die Erstellung moderner Unterrichtsmaterialien und Arbeitsblätter durch Lehrkräfte die digitale Nutzung von Lehrbuchteilen, beispielsweise von Tabellen, Quellentexten und Schaubildern“ (Sawall www.golem.de 07.05.2012; SZ 05./06.05.2012, 10).

Bund

Tiermast-Datenbank beschlossen

Die Agrarminister des Bundes und der Länder haben auf ihrer Frühjahrskonferenz April 2012 in Konstanz beschlossen, eine bundesweite Datenbank zur Eindämmung des Antibiotika-Missbrauchs in der Tiermast einzurichten. Im Arzneimittelgesetz soll die Möglichkeit für den Aufbau der Datenbank geschaffen werden, so Landwirtschafts- und Verbraucherministerin Ilse Aigner (CSU): „Es ist unser gemeinsames Ziel, die Anwendung von Antibiotika in der Nutztierhaltung auf das absolut notwendige Maß zu beschränken.“ Zuvor hatte sich ihr Ministerium jahrelang einer solchen Datenbank und der damit verbundenen Erfassung der Tierärzte und der Betriebe mit dem Argument des Datenschutzes verweigert (SZ 28./29.04.2012, 25).

Bayern

BayLDA prüft automatisiert Google Analytics

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat 13.404 Sites bayerischer Betreiber daraufhin überprüft, ob diese Google Analytics datenschutzkonform einsetzen. Ob ein solcher rechtskonformer Einsatz von Analytics überhaupt möglich ist, ist unter den Datenschutzbehörden umstritten. Von den geprüften Seiten hatten 2.449 das Analyse-Tool eingesetzt und von diesen hielten wiederum nur 3% die vom BayLDA geforderten Richtlinien zum Datenschutz ein. 2.371 Site-Betreiber werden nun schriftlich aufgefordert, ihre Webpräsenzen rechtskonform zu gestalten. Von einem Bußgeld will das Amt aber absehen. Andreas Sachs, Referatsleiter IT-Sicherheit und technischer Datenschutz bei der bayerischen Aufsichtsbehörde erläuterte: „Uns geht es vornehmlich darum, auf den Missstand hinzuweisen und auf die Einhaltung hinzuwirken.“ Sollten sich angeschriebene Firmen nachhaltig verweigern, seien auch Bußgelder möglich. Diese können bis zu 50.000 Euro betragen.

Bayern ist nicht das erste Bundesland, das die Einhaltung der Vorgaben beim Einsatz von Google Analytics überprüft. Schon 2008 beanstandete das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD), dass Analytics in seiner Grundstruktur den Datenschutzregeln widerspricht. Bei einer Stichprobe Anfang 2011 in Rheinland-Pfalz fehlte bei den meisten der überprüften Sites die erforderliche Information, dass Google Analytics eingesetzt wird. Aufgrund eines Beschlusses des Düsseldorfer Kreises, dem bundesweiten Gremium der Aufsichtsbehörden für den Datenschutz, müssen Site-Betreiber in ihren Datenschutzhinweisen auf das von Google bereitgestellte Deaktivierungs-Add-On hinweisen. Auch müssen die Site-Betreiber Google mit der Kürzung der IP-Adresse beauftragen. Jeder Homepage-Betreiber muss außerdem mit Google einen schriftlichen Vertrag über Auftragsdatenverarbeitung schließen (Kaufmann www.heise.de

08.05.2012; ULD www.datenschutzzentrum.de/tracking/; BayLDA PE 07.05.2012).

Bayern

Polizeiliche Nacktkontrollen in der Kritik

Die öffentliche Kritik an entwürdigenden polizeilichen Ganzkörperkontrollen bei vermeintlichen Drogenbesitzern in der bayerischen Landeshauptstadt München nimmt zu. So war vor 5 Jahren ein damals 22jähriger von der Polizei mit einigen Hanfblättern, allerdings ohne das berauschende THC, angetroffen worden. Ein Verfahren wegen Verstoß gegen das Betäubungsmittelgesetz wurde eingestellt, nicht jedoch der Vorwurf im Polizeicomputer gelöscht. Seitdem wird dieser Mann immer wieder von der Polizei kontrolliert und wurde in 10 Fällen gezwungen, sich völlig nackt auszuziehen, sich breitbeinig hinzustellen und zu bücken, verbunden mit einer Analnachschau. Vor den Augen der Polizisten musste er die Vorhaut des Penis zurückziehen. Drogen gefunden haben die Beamten bei ihm noch kein einziges Mal. Regelmäßig wurde ihm nicht erlaubt einen Anwalt anzurufen. Als der Betroffene einmal in seiner ohnmächtigen Wut die Beamten als „Staatsbimbos" beschimpfte, wurde er wegen Beamtenbeleidigung angeklagt, aber vom Gericht freigesprochen. Sein Rechtsanwalt Dirk Thöle berichtete: „Richterin und Staatsanwältin waren schockiert über das Verhalten der Polizeibeamten." Im Prozess habe ein Beamter ausgesagt, diese Art der Kontrolle sei üblich: „Das machen wir immer so."

Polizeisprecher Wolfgang Wenger rechtfertigte das polizeiliche Vorgehen: „Die Kontrolle von Personen erfolgt immer nach Erfahrungswerten der Beamten." Eine derartige „Kontrolltiefe" sei aber „generell nicht üblich". Die „Inaugenscheinnahme des Intimbereichs" sei rechtlich zulässig, wenn „drogentypische Auffälligkeiten sowie polizeilich einschlägige Vorerkenntnisse" gegeben seien: „Grundsätzlich sind polizeiliche Durchsuchungen rechtmäßig, wenn Tatsachen die Annahme rechtfertigen, dass die Person Sachen mit sich führt, die sichergestellt werden dürfen." Warum der Betroffene bereits zehn Mal auf diese Weise kontrolliert wurde, konnte Wenger nicht sagen: „Er scheint in ein bestimmtes Raster zu fallen". Ob der Betroffene tatsächlich Drogen konsumiert, wurde nie untersucht, einem Drogentest musste er sich nie unterziehen (Wimmer, SZ 07.05.2012, 30).

Brandenburg

Angebliche Datenschützer rufen illegal an und betrügen

Die Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg (LDA Bbg) Dagmar Hartge warnte mal wieder vor unverlangten Telefonanrufen, bei denen die Anrufenden vorgeben, für eine „Verwaltungszentrale für Datenschutz" tätig zu sein. Sie behaupten, die Angerufenen hätten an einem Gewinnspiel teilgenommen. Unter dem Vorwand, die persönlichen Daten der Betroffenen schützen und die angebliche Teilnahme am Gewinnspiel beenden zu wollen, fragen die Anrufenden oftmals nach den Bankverbindungsdaten, um Geld von den Konten der Angerufenen abzubuchen.

Die LDA Bbg wies darauf hin, dass eine „Verwaltungszentrale für Datenschutz" nicht existiert. Mit dieser Bezeichnung solle offenbar der Anschein von Seriosität erweckt werden. Derartige Anrufe dienen missbräuchlichen Zwecken. Die Datenschutzbeauftragten von Bund und Ländern riefen nicht von sich aus BürgerInnen an, um ihre Hilfe anzubieten. Deshalb empfiehlt die LDA Bbg: „Geben Sie Ihre persönlichen Daten, insbesondere Anschrift und Kontoverbindung, nicht an unseriöse Anrufer heraus. Notieren Sie die Nummer des Anrufenden und beenden Sie das Gespräch umgehend. Machen Sie von Ihren Widerrufsrechten Gebrauch, falls durch ein solches Telefonat bereits ein Vertrag zustande gekommen ist und fordern Sie die Löschung Ihrer Daten. Kontrollieren Sie die Bewegungen auf Ihrem Konto, um gegebenenfalls einer unberechtigten Lastschrift rechtzeitig widersprechen zu können. Liegen Anhaltspunkte für ein strafbares Verhalten vor, sollten die Strafverfolgungsbehörden, die örtliche Polizeidienststelle oder aber die Staatsanwaltschaft informiert werden." Wer auf unseriöse Anrufe hereingefallen ist, könne sich an die Verbraucherzentralen wenden. Die Bundesnetzagentur geht unerlaubter Telefonwerbung und Rufnummernmissbrauch nach und informiert darüber auf ihrer Internetseite (http://www.bundesnetzagentur.de/cln_1932/DE/Verbraucher/RufnummernmissbrauchSpamDialer/RufnummernmissbrauchSpamDialer_node.html; PE LDA Bbg 15.05.2012).

Hamburg

Bürgermeister Scholz für Facebook und gegen Verbraucherdatenschutz

Der Bürgermeister der Hansestadt Hamburg Olaf Scholz zeigte auf einer Veranstaltung, die das Unternehmen Facebook gemeinsam mit einem Reiseveranstalter für Kitesurfer veranstaltete, dass er wenig Verständnis für die Angst vor Facebook als übermächtigem Datensammler habe: „Ich bin davon überzeugt, dass die positiven Aspekte bedeutender sind als die negativen.". Der SPD-Politiker widersprach den Bedenken von Verbraucher- und Datenschützern mit dem Hinweis, nicht die Unternehmen, sondern der Gesetzgeber sei für den Verbraucherschutz zuständig: „Wir müssen die rechtlichen Grundlagen schaffen, dass die Leute solchen Diensten vertrauen können." In Hamburg sitzt der kleine Deutschland-Ableger des großen Facebook-Konzerns. Um die Ansiedlung der deutschen Niederlassung hatten sich auch andere Großstädte wie Berlin bemüht. Scholz profilierte sich bei dem PR-Termin am 18.04.2012 mit ungetrübtem Fortschrittsoptimismus und wies Vorbehalte, die auch andere PolitikerInnen gegenüber Facebook hegen, zurück: „Ich habe mich als erster Bürgermeister darum gekümmert, die sozialen Netzwerke ins Rathaus zu holen". Die in den Netzwerken praktizierte

Kommunikation sei für die Demokratie sehr wichtig. Er sei der für Facebook „zuständige Senator". Auf die Frage, ob er wisse, wie man bei Facebook verhindert, auf unvorteilhaften Fotos verlinkt zu werden, gestand er: „Ich weiß zumindest, wie ich es herausbekommen könnte. Aber ich betreue meine Seite auch nicht selbst" (www.heise.de 19.04.2012).

Hessen

Verkabelter Prüfling betrügt bei Führerscheintest

Ein Fahrschüler aus Siegen soll einer mit ihm zusammenarbeitenden Betrügerbande 1.000 Euro dafür bezahlt haben, dass diese ihn bei seiner Theorieprüfung für den Führerschein unerlaubt hilft. Die Helfer verkabelten den 23jährigen und gaben ihm von ihrem Versteck in einem Lastwagen aus Tipps. Eine Kamera übertrug den Fragebogen vom Computerbildschirm an die Helfenden, die wiederum per Handyverbindung und Minikopfhörer die richtigen Antworten zuflüsterten. Der Schwindel flog auf; die Polizei trennte die Verbindung. Am Ende hatte der allein gelassene Prüfling 95 Fehlerpunkte. Er darf den Test erst nach einer Sperrfirst wiederholen (SZ 08.05.2012, 10).

Hessen

Internetbelästigte Friedrich belästigt zurück

Die Hochspringerin Ariane Friedrich war bisher vor allem dafür prominent, dass sie 2009 die Hallen-Europameisterschaft gewann und mit einer übersprungenen Höhe von 2,06 Metern deutsche Rekordhalterin ist. Als sie nun einen angeblichen Stalker, genauer Web-Attacker, mit vollem Namen und Wohnort per Facebook outete, löste sie eine breite Debatte aus: Darf sie das? Soziale Netzwerke sind für Prominente eine gute Möglichkeit, direkt mit ihren Fans in Kontakt zu treten und zu kommunizieren. Viele PolitikerInnen, SportlerInnen, SängerInnen oder SchauspielerInnen betreiben öffentliche Facebook-Seiten: UserInnen können mit einem Klick auf „Gefällt mir" Statusmeldungen und Fotos der Stars abonnieren. Diese Seiten sind immer öffentlich, jedeR kann sie ansehen, auch wenn er nicht „Gefällt mir" geklickt hat.

Die Hochspringerin Ariane Friedrich hat eine solche Facebook-Seite. Dort schrieb sie bisher über eher unspektakuläre Themen. Am 16.04.2012 postete sie dann aber auf ihrer Pinnwand: „Liebe Followers, eben erreichte mich folgende Facebook-Mail." Dann nennt sie den vollen Namen und den Wohnort eines Mannes. Er soll ihr geschrieben haben: „Willst du mal einen schönen Schwanz sehen, Gerade geduscht und frisch rasiert." Zusätzlich habe er noch eine Datei mitgeschickt, „die ich nicht öffnen werde (...). Ich möchte weder Ihr Geschlechtsteil, noch die Geschlechtsteile anderer Fans sehen. Anzeige folgt." Diese Statusangabe löste eine wilde Debatte im Netz und in klassischen Medien aus: Ist es moralisch vertretbar, sich auf diese Weise öffentlich gegen Belästigungen zu wehren, oder schafft Ariane Friedrich damit einen digitalen Pranger und greift gar zur Selbstjustiz?

Die Internetdebatte

Tausende Menschen klickten bei Friedrichs Statusmeldung auf „Gefällt mir", über 1000 Kommentare wurden abgegeben, v. a. mit Zustimmung zum Vorgehen der Hochspringerin: „Ich bewundere Ihren Mut. Weiter so", „Zeig´s dem Drecksack" und „Vielleicht ist das für andere Stalker eine Warnung." Man solle „jeden, der sich sexuell an Frauen vergreift, öffentlich an den Pranger stellen." Man müsse „dem perversen Schwein mal einen Besuch abstatten." Doch es gab auch viele kritische Stimmen: „Selbstjustiz ist strafbar.", „Um Himmels willen, löschen Sie doch mal die Adresse." „Sind wir wieder im Mittelalter angekommen?" Boulevardmedien machten sich sogleich auf die Suche nach dem Mail-Absender.

Die Debatte wurde erbitterter, als Friedrich kurz danach einen zweiten, sehr viel längeren Eintrag folgen ließ. Dort rechtfertigt sie ihr Vorgehen gegen die KritikerInnen: „Es gibt einfach einen Punkt, an dem Schluss ist". Sie habe schon öfter solche Mails erhalten und nun die Nase voll: „Ich wurde in der Vergangenheit beleidigt, sexuell belästigt, und einen Stalker hatte ich auch schon. Es ist Zeit zu handeln, es ist Zeit, mich zu wehren. Und das tue ich. Nicht mehr und nicht weniger." Sie sei nicht mehr bereit, sich „doppelt zum Opfer zu machen und stets zu schweigen." Die umstrittene Nennung von Namen und Wohnort findet sie gerechtfertigt: „Ich habe mich weder mit der Veröffentlichung seines Namens strafbar gemacht, noch versucht, ihm Unrecht anzutun."

Damit ging die Diskussion erst richtig los. Dieser Beitrag gefiel wieder umgehend tausenden von Mitgliedern, und mehr als 2.300 hinterließen einen Kommentar. Diesmal allerdings wurde der Ton schärfer, und die Zweifel nahmen zu, ob Friedrich richtig gehandelt hat. Viele NutzerInnen fragen, ob denn der genannte Mann zweifelsfrei hinter der obszönen Mail steckt. Es könne ja auch sein, dass jemand unter falschem Namen eine Nachricht geschickt habe. Andere geben zu bedenken, dass auch mögliche Namensvettern beschuldigt würden. Jemand schreibt: „Es gibt noch mindestens einen zweiten T.D. aus A."

Internetnutzende fühlten sich offenbar angestachelt, die Identität des Mannes herauszufinden. Sie verlinkten auf ein Facebook-Profil mit dem Namen und dem genannten Ort, inzwischen wurde es gelöscht. Und auch wenn es bundesweit mehrere Gemeinden und Ortsteile mit dem Namen gibt, wollen einige den „echten" herausgefunden haben. Im Gästebuch der Webseite eines gleichnamigen Ortsteils hinterließen Besucher Warnungen vor dem angeblichen „Perversling". Dort hieß es auch: „Schützt Eure Kinder vor ihm!!!" Der Webmaster hat diese Einträge inzwischen gelöscht, er schreibt im Gästebuch: „Ich bitte darum, Einträge über Personen unseres Ortes zu unterlassen." Nach Rundfunkangaben hatten sich Neugierige bei Dorfbewohnern nach dem Mann erkundigt. Menschen mit extremen Ansichten meldeten sich zu Wort – sie meinten, dass jemand, der so etwas schreibt, auch Kinder vergewaltigen könnte. Andere wieder fanden eine solche Ansicht „unerträglich" und mahnten zur Besonnenheit. Wenn man eine solche Mail als Stalking oder

sexuelle Gewalt bezeichne, verharmlose man beides. Viele Mitglieder fühlten sich an Emden erinnert: Die Polizei hatte dort nach dem Mord an einer Elfjährigen einen Unschuldigen verhaftet; via Facebook hatten manche zur Lynchjustiz aufgerufen – und sich vor dem Polizeigebäude getroffen.

An die Adresse von Ariane Friedrich und der Befürworter ihrer Aktion schreibt ein Facebook-Mitglied: „Mir graut vor Deutschland, wenn ich diesen Mob lese (…) Hier richten Hunderte die soziale Existenz unbeteiligter Menschen, die auf Grund zufälliger Namensgleichheit und miserabler Recherche von Frau Friedrich an den Pranger gestellt werden, zu Grunde." Andere sprachen von „moderner Hexenjagd." Manche fanden auch, dass die 28jährige als öffentliche Person Vorbildcharakter haben müsse – insbesondere, da sie studierte Polizeikommissarin ist. Ein User meinte: „Hat eine ausgebildete Polizistin wirklich so wenig Vertrauen in den Rechtsstaat, auf den sie ihren Amtseid geleistet hat, dass sie wirklich glaubt, zu solchen Mitteln greifen zu müssen?"

Fachleute kommen zu Wort

Als die Sache weitere mediale Aufmerksamkeit auslöste, meldeten sich „ExpertInnen". Rechtsanwalt Udo Vetter meinte in seinem bekannten „Lawblog": „Persönlichkeitsrechte? Datenschutz? Viel kann die Polizeikommissarin und Spitzensportlerin Ariane Friedrich darüber in ihrer Ausbildung nicht gelernt haben. Sonst würde die Hochspringerin nicht auf die Idee kommen, die persönlichen Daten eines Mannes zu veröffentlichen, der ihr eine anzügliche Mail geschickt hat. ... Man muss sich nur mal vorstellen, dass der Absender der Mail gefälscht ist. Das könnte dann sehr, sehr teuer für Frau Friedrich werden. Aber selbst wenn es tatsächlich den ´Richtigen` trifft – was Friedrich zu beweisen hätte –, ist das An-den-Pranger-stellen unrechtmäßig. Wenn der Betroffene zum Anwalt geht, kann das immer noch ziemlich teuer und unangenehm für die Kommissarin werden." Der Medienrechtler Thomas Hoeren sah in Friedrichs Verhalten „einen klaren Verstoß gegen das Persönlichkeitsrecht". Auch die Mail eines Stalkers falle unter das Briefgeheimnis. Mit der Veröffentlichung habe Friedrich ihre Sorgfaltspflicht verletzt.

Wenn die obszöne Mail tatsächlich von dem Mann stammte, hat Friedrich keine falschen Tatsachen behauptet und kann wohl strafrechtlich nicht belangt werden. Doch selbst unter dieser Voraussetzung ist nicht ausgeschlossen, dass der Mann zivilrechtlich Schadensersatzansprüche geltend machen könnte wegen der Verletzung seiner Persönlichkeitsrecht durch die Namens- und Wohnortnennung.

Dem widersprach Netzexpertin Anke Domscheit-Berg. Manchmal könne Namensouting das einzige Mittel sein, um sich gegen Cyber-Mobbing zu wehren, etwa bei Stalkern, die man einfach nicht loswerde. Wenn es wie hier aber nur um eine einzige Mail gehe, sei dies „übertrieben" und ein „unüberlegter Schnellschuss": „Was passiert, wenn Fans gegen den Mann aktiv werden?" Datenschützer Thilo Weichert meinte: „Friedrich und auch ihren PR-Managern mangelt es offenbar an Medienkompetenz." Sie habe die Reaktion auf ihren Post unterschätzt. Schuld daran trage aber auch Facebook, das den „Exhibitionismus der Nutzer" befeuere, um möglichst viele Daten zu sammeln. Er erwarte für die Zukunft „weitere gefährliche Exzesse".

Helmut Markwort, Herausgeber des Focus, meinte nicht differenzieren zu müssen und stellte sich auf die Seite von Friedrich: „In der Debatte um das durch Ariane Friedrich erzwungene Outing fällt auf, dass viele Teilnehmer sich wieder einmal rücksichtsvoll mit dem Täter beschäftigen und das Opfer wegen seines Vorgehens angreifen. Die mutige Sportlerin hat mit ihrem Schritt auf jeden Fall ein wichtiges Signal gezündet und sicher Opfer ermutigt und Täter hoffentlich eingeschüchtert. Die resignierende Haltung, das Netz sei eben ein rechtsfreier Raum, darf sich weder in den Köpfen noch im Alltag durchsetzen."

Der berliner Medienanwalt Christian Scherz bewertete den Fall etwas realistischer und weniger heroisch: „Ihr Verhalten ist grenzwertig, für mich ist es trotzdem nachvollziehbar. Friedrichs Aktion war ein Hilfeschrei. Hier hat sich eine Person gewehrt, da der Staat und der Gesetzgeber nicht wirklich helfen. Natürlich hätte sie es dabei belassen sollen, gegen den Absender Anzeige zu erstatten. Nur oftmals führt das nicht weiter. Ich vertrete viele Prominente, aber auch ganz normale Bürger, die monatelang über das Internet diffamiert werden. Jeder dritte Jugendliche ist Opfer von Internetmobbing. In unseren Fällen haben Anzeigen selten dazu geführt, dass der Täter überführt, geschweige denn bestraft wurde. Am Fall Friedrich kann man beobachten, welchen unfassbar rauen Ton diese Thematik des fehlendes Schutzes des Individuums in der digitalen Welt schon angenommen hat. Das klingt vielleicht ein bisschen altmodisch, aber ich rate meinen Klienten dazu, sich gut zu überlegen, wie offen sie sich im Netz präsentieren, da man damit auch Angriffsflächen schafft. Das Ziel muss doch sein, Regeln zu finden. ... Das ist eine der größten Herausforderungen, vor denen wir in der Kommunikationskultur in den nächsten Jahren stehen werden."

Weitere Folgen

Nachdem die öffentliche Diskussion nicht enden wollte, erklärte Günter Eisinger, Trainer von Friedrich, dass es keine Interviews, keine schriftliche Stellungnahme, nicht mal mehr ein Zitat von der Sportlerin zu der Sache geben werde. Wenige Monate vor den Olympischen Spielen in London gebe es für sie wichtigere Dinge. Als einziges Zitat ließ Eisinger dann doch einen Satz zu: „Wir raten allen Nutzern von Facebook, sorgsam damit umzugehen." Die hessische Polizei nahm strafrechtliche Ermittlungen auf und wertete dafür das gesamte Facebook-Profil aus. Ein Sprecher des Landeskriminalamtes (LKA) meinte: „Es gibt noch mehrere Sachen, die möglicherweise zum Nachteil von Frau Friedrich strafrechtlich relevant sind. Es geht in Richtung Beleidigung." Er bestätigte, dass gegen Friedrich mehrere Strafanzeigen vorliegen. Die Staatsanwaltschaft Darmstadt hat schon Anzeigen wegen der „Beschuldigung eines Unschuldigen" zurückgewiesen. Friedrichs Dienstherr, die hessische Bereitschaftspolizei, prüfte die Einleitung eines Disziplinarverfahrens. Ermittelt wird durch die Staatsanwaltschaft Marburg auch gegen den mutmaßlichen Cyber-Stalker.

Der Verdacht richtet sich gegen einen 38jährigen, dessen Haus durchsucht worden ist. Die dabei sichergestellten Datenträger werden daraufhin ausgewertet, ob es Hinweise gibt auf „Beleidigung“ oder das „Verbreiten pornografischer Schriften.“ Der Geoutete hat bisher keine Schritte gegen Friedrich eingeleitet. Friedrichs Manager berichtete, dass die Athletin sich mit dem mutmaßlichen Belästiger treffen möchte (Graff, SZ 24.04.2012, 9; Frickel www.focus.de 24.04.2012; www.fr-online.de 25.04.2012; Staudinger SZ 05./06.05.2012, 14; Weddeling, Markwort, Focus 18/2012, 51, 166; Der Spiegel 18/2012, 139).

Schleswig-Holstein

Schüler ändern Noten auf dem Schulrechner

Zwei 19jährige Gymnasiasten in Lübeck haben sich in den Computer ihrer Schule, dem Johanneum, gehackt und versucht, ihre Abiturnoten zu manipulieren. Aufgeflogen ist der Fall, als sich die Schüler zur Abi-Prüfung anmeldeten und dabei auffiel, dass die Punktzahlen der schriftlichen Leistungsnachweise von denen in der Schuldatenbank abwichen. Die Schüler waren Mitglied einer Arbeitsgruppe aus SchülerInnen, Lehrkräften und Software-Experten, die das interne Schulnetzwerk benutzerfreundlich gestalten sollte. Über das Netzwerk soll das Benutzen und Einbinden von Laptops im gesamten Johanneum ermöglicht werden – inklusive kabellosem Internetzugang.Sie nutzten ihre Kenntnisse, um für ihre Zwecke den Schulrechner zu manipulieren.

Schulleiter Rüdiger Bleich bestätigte: „Sie waren zum Teil mit der Netzinstallation beschäftigt“ So seien sie in internen Bereichen unterwegs gewesen, aber nicht in sensiblen Arealen. „Sie hatten keine Codes oder Passwörter.“ Diese mussten sie aber kennen, um sich den Zugang zu der Notendatenbank zu verschaffen. Nach Angaben von Bleich versuchten die Junghacker, von Schulrechnern auf die zentrale Datenbank zuzugreifen. Schulrat Helge Daugs meinte, dies sei der erste derartige Angriff in Lübeck. Er schließe ähnliche Versuche aus. Daugs: „Die Schülerdaten sind von den Lehrkräften ausschließlich auf verschlüsselten Datenträgern zu transportieren, und die Verwaltungsrechner mit Schülerdaten dürfen via offenem Internet nicht zu erreichen sein.“ Dem widersprach der Datenschutzbeauftragte des Landes Schleswig-Holstein Thilo Weichert: „Dies ist der erste Fall, der uns bekannt geworden ist, ich bin aber sicher, dass solche Attacken in der Vergangenheit unerkannt durchgeführt wurden und auch künftig durchgeführt werden. Die Abschottung des Schulnetzwerkes war völlig unzureichend.“ Er forderte das Bildungsministerium auf, endlich den Schulen einheitliche IT-Sicherheitsstandards an die Hand zu geben. Der Sprecher des Bildungsministeriums Thomas Schunck, erklärte: „Wir werden die Vorgänge prüfen und unsere Lehren daraus ziehen.“

Die Jungs müssen sich nun wegen Datenausspähen und -manipulation verantworten. Womöglich könnte alles aber auch, so Staatsanwalt Günter Möller, als „jugendliche Überschwangshandlung“ gewertet werden. Dann würde das Verfahren unter Auflagen eingestellt – etwa gegen Zahlung einer Geldstrafe. Durch den vorzeitigen Abgang vom Johanneum haben die 19-Jährigen lediglich die Fachhochschulreife, das Abitur können sie später aber nachholen (www.ln-online.de 11.05.2012; Hellerling www.ln-online.de 12.05.2012, KN 12.05.2012, 15).

Datenschutznachrichten aus dem Ausland

Europa

Fluggastdaten-Transfer in die USA abgesegnet

Die Entscheidung

Das Parlament der Europäischen Union (EU) hat am 19.04.2012 mit klarer Mehrheit für das umstrittene transatlantische Abkommen zum Transfer von Flugpassagierdaten gestimmt. 409 Abgeordnete votierten für das Vorhaben, 226 dagegen. Die USA dürfen damit Passenger Name Records (PNR) weiterhin zunächst 15 Jahre speichern. Angeblich anonymisiert dürfen die Informationen der Fluggesellschaften unbegrenzt aufbewahrt werden. US-Behörden können damit auf PNR aller Fluglinien mit Sitz in Europa oder den USA zugreifen, um Straftaten zu verhindern oder zu verfolgen, auf die in den Vereinigten Staaten drei Jahre Haft stehen. Dazu zählt etwa auch Diebstahl. Schwerpunktmäßig soll der Vertrag helfen, terroristische und schwere Kriminalität zu bekämpfen.

Die Abgeordneten folgten einer Empfehlung des federführenden Innenausschusses, nicht aber der Berichterstatterin Sophie in‘t Veld. Diese hatte in ihrer Vorlage zu bedenken gegeben, dass viele der Kriterien, die das Parlament zunächst selbst aufgestellt hatte, „nicht zufriedenstellend eingehalten“ werden. Nicht nur sei die Speicherdauer der Daten, zu denen auch Kreditkarten- und Telefonnummern, IP-Adressen oder besondere Speisewünsche zählen, faktisch auf „unendlich“ hochgeschraubt worden. Zudem könne das Department of Homeland Security (DHS) weiterhin automatisch abgleichen sowie Rasterfahndungen durchführen und personenbezogene Profile erstellen. Auch sei der Rechtsschutz für EU-BürgerInnen unzureichend.

Die Debatte

Der Abstimmung war eine sehr kontroverse Debatte vorausgegangen.

„Grundrechte sind nicht verhandelbar“, meinte die Niederländerin in‘t Veld. Die vorgesehene Kontrolle durch Brüssel sei „ein Witz“. Schon derzeit zögen US-Behörden täglich bis zu 82.000-mal am Tag Daten aus den Reservierungssystemen der Fluglinien ab. Daran werde sich mit der Übereinkunft wenig ändern. Zudem würden künftig viele andere Länder einschließlich China oder Saudi-Arabien nach denselben Zugriffsrechten fragen. Sowohl der EU-Datenschutzbeauftragte Peter Hustinx als auch die Artikel-29-Gruppe der europäischen Datenschutzbehörden hatten zuvor deutlich gemacht, dass das Verhandlungsergebnis nicht den hiesigen Grundrechten gerecht werde.

EU-Innenkommissarin Cecilia Malmström erkannte an, dass es sich für die Abgeordneten um eine „schwierige Entscheidung“ handle. Das Ergebnis der Absprachen sei „nicht hundertprozentig perfekt“. Zwischen den USA und der EU sei aber ein „Geben und Nehmen“ nötig. Weitere Verhandlungen mit Washington stellten keine Option dar. Die USA sammelten zudem ohnehin die begehrten Fluginformationen, was aber ohne die Vereinbarung zu einem rechtlichen Freiraum und in Folge zu Klagen von Reisenden führen könne. Im Namen der konservativen Fraktion der Europäischen Volkspartei (EVP) betonte der CDU-Parlamentarier Axel Voss, dass er die Kritik an der Übereinkunft in vielen Bereichen nachvollziehen könne. Es sei aber erforderlich, Verantwortung zu übernehmen und sich nicht auf ideologische Standpunkte zurückzuziehen. „Die USA sind unser Partner im Kampf gegen den Terror, wir profitieren von den Auswertungsergebnissen“, ergänzte sein Fraktionskollege Manfred Weber (CSU).

Gespalten präsentierten sich die Sozialdemokraten. Eine knappe Mehrheit der Fraktion sei für das Abkommen, erläuterte der britische Labour-Abgeordnete Claude Moraes. Es gebe Verbesserungen im Vergleich zu früheren Versionen. Wichtig sei nun, die Umsetzung und die geplanten Überprüfungen abzuwarten. Die SPD-Abgeordnete Birgit Sippel kritisierte dagegen, dass Datenschutzbeauftragte bei der Evaluation nicht beteiligt werden sollen. Der Vertrag stelle alle BürgerInnen unter Generalverdacht. Keine gemeinsame Linie vertraten auch die Liberalen. Der FDP-Abgeordnete Alexander Alvaro konstatierte, dass das vage Abkommen keinen gerechten Ausgleich zwischen Sicherheit und Freiheitsrechten mit sich bringe. Eine britische Liberale unterstützte dagegen voll und ganz den Kurs Malmströms.

Jan Philipp Albrecht, Innenexperte der Grünen, warnte vor einem „offenen Rechtsbruch“. Der Vertrag erlaube einen automatisierten Datenabgleich mit Gefahrenprofilen. Die vorgesehene „Vorratsdatenspeicherung von bis zu 15 Jahren“ sei nicht verhältnismäßig: „Die heutige Entscheidung von Konservativen und Sozialdemokraten für das Fluggastabkommen mit den USA ist ein weiterer Schritt in den Überwachungsstaat. Zum ersten Mal hatte das Europäische Parlament die Chance, die langjährige und anlasslose Rasterfahndung und Vorratsdatenspeicherung aller USA-Reisenden zu stoppen, doch die Mehrheit hat sie nicht genutzt.“ Cornelia Ernst von den Linken sieht das „elementare Recht auf den Schutz personenbezogener Daten ausgehebelt“. Es gebe keinen ernstzunehmenden Rechtsbehelf, vielmehr werde eine „Rechtsbehinderung“ daraus.

Rechtsgutachten: Verstoß gegen EU-Recht

Kurz vor der Abstimmung versuchten die Grünen noch mit einem von ihnen in Auftrag gegebenen Rechtsgutachten die positiv eingestellten EU-Abgeordneten umzustimmen. Das Gutachten des Passauer IT-Rechtlers Gerrit Hornung und der Luxemburger Sicherheitsforscherin Franziska Boehmbringe kommt zu dem Ergebnis, dass der neue Text nur „sehr wenige Verbesserungen“ gegenüber den Fassungen von 2004 und 2007 mit sich bringt; in mehreren Bereichen würden die Datenschutzstandards hingegen abgesenkt. Die Anforderungen des EU-Parlaments würden nicht ausreichend berücksichtigt. PNR könnten für Zwecke verwendet werden, die nichts mit Terrorismus oder schweren internationalen Straftaten zu tun hätten. Die Speicherfristen seien – gerade bei eigentlich Unverdächtigen – ins Unendliche ausgeweitet worden. Die neue vage Vorgabe einer „Anonymisierung“ mit späteren Möglichkeiten zur „erneuten Personalisierung“ führe allein zu Rechtsunsicherheit. EU-BürgerInnen bekämen nach wie vor keine ausreichenden Mittel in die Hand, um ihre Rechte in den USA durchzusetzen. Auch bleibe der von der EU-Kommission ausgehandelte Vertrag hinter deren Initiative für eine Richtlinie zum Datenschutz im Sicherheitsbereich zurück. Die Probleme beim Schutz der Privatsphäre der EU-BürgerInnen bleiben nach Meinung der Gutachtenden nicht nur erhalten, sondern würden in einigen Bereichen noch verschärft. Dem stünden leichte Fortschritte wie die Verschärfung der Bedingungen für den PNR-Transfer in Drittstaaten gegenüber. Aber selbst hier habe das Parlament auf noch höhere Hürden gedrängt. Das Abkommen verletze EU-Recht.

Der Berliner Datenschutzbeauftragte Alexander Dix wies nach der Zustimmung zu dem Abkommen darauf hin, dass das Bundesverfassungsgericht (BVerfG) 2010 bei seiner Verfassungswidrigkeitserklärung der Vorratsdatenspeicherung darauf hingewiesen hat, dass der „Spielraum für weitere anlasslose Datensammlungen auch über den Weg der Europäischen Union erheblich geringer“ wird. Vor diesem Hintergrund sei es nicht ausgeschlossen, dass das BVerfG wie auch der Europäische Gerichtshof sowohl die Vorratsdatenspeicherung wie auch die Fluggastdatenspeicherung erneut überprüfen: „Das Maß ist jetzt voll.“

Dass PNR unbescholtene Menschen treffen kann, zeigt die Geschichte von Paul-Emile Dupret, Berater der Linksfraktion des EU-Parlaments. Er steht auf einer No-Fly-Liste der USA und darf nicht in die USA fliegen, ohne dass er weiß, weshalb. Offensichtlich ergaben die PNR-Daten ein Profil, das Dupret verdächtig erscheinen lässt. Ein Direktflug zwischen Paris und Mexiko, bei dem ohne Landung die USA nur überflogen werden sollte, musste wegen der Verdachtsspeicherung von Dupret umgeleitet werden (DANA 3/2009, 116; Krempl www.heise.de 14.03.2012; Beuth www.zeit.de 14.03.2012; Krempl www.heise.de 19.04.2012; PM Albrecht MdEP 19.04.2012; PE BlnBDI 25.04.2012); siehe auch die Datenliste auf Seite 100.

Europa

PNR-Erfassung jetzt auch bald in der EU?

Kurz nach der Entscheidung des Parlaments der Europäischen Union (EU) zum Vertrag mit den USA am 19.04.2012 (s. o.) haben die EU-Innenminister am 26.04.2012 eine politische Einigung über einen Vorschlag der EU-Kommission hergestellt, wonach auch Fluggastdaten nicht nur von Flügen aus Drittstaaten in die EU, sondern auch innerhalb der EU fünf Jahre lang gespeichert werden sollen. Keine Einigkeit besteht, ob tatsächlich alle „Binnenflüge erfasst werden sollen. Vorerst einigte man sich darauf, dass das den einzelnen Ländern überlassen bleiben soll. Von Sicherheitsleuten wird dies allerdings für unpraktikabel abgelehnt. Großbritannien tritt vehement dafür ein, alle Binnenflüge zu erfassen. Gemäß der nun erfolgten Einigung sollen die Daten zwei Jahre „unmaskiert" gespeichert werden. Der ursprüngliche Entwurf für eine Richtlinie der EU-Kommission sah eine sogenannte Anonymisierung der Daten bereits nach 30 Tagen vor. Insgesamt sollen die Informationen fünf Jahre lang vorgehalten werden können. Auch nach den ersten zwei Jahren würde es etwa beim Verdacht auf schwere oder terroristische Straftaten möglich sein, Rückschlüsse auf einzelne Personen zu ziehen.

Vorlage für die Einigung war ein Vorschlag der dänischen Ratspräsidentschaft, der als Kompromiss eine Optionsmöglichkeit der Mitgliedstaaten vorsah. Die Kommission plädierte zunächst dafür, nur Flüge von und nach Europa aus dem Ausland zu erfassen. Der Rat der EU drängte dagegen darauf, die Initiative auszuweiten. Bleiben soll es dabei, 19 Datenkategorien zu erheben. Dazu gehören neben Name, E-Mail-Adresse, Telefon-, Konten- und Kreditkartennummern, aber auch Essenswünsche. Direkte Fischzüge der Strafverfolger in den Buchungssystemen der Fluglinien sowie Rasterfahndungen in den Beständen sollen ausgeschlossen werden.

2008 hatte die Bundesregierung einen früheren Plan für ein vergleichbares System mit Speicherfristen bis zu 13 Jahren zu Fall gebracht. Bundesinnenminister Hans-Peter Friedrich beteiligte sich dieses Mal nicht an der Debatte. Der CSU-Politiker ließ durchblicken, dass er dies als Enthaltung verstanden wissen wolle. Bundesjustizministerin Sabine Leutheusser (FDP) erklärte von Anfang an ihre Ablehnung der geplanten Regelung. Später erklärte auch Friedrich, das Konzept der EU sei „sehr weitreichend": „Wir werden sehr genau prüfen müssen, ob wir ein solches System wirklich brauchen." Je mehr es aber Visa-Freiheit gebe, desto wichtiger würden „Ersatzinstrumente", um die Sicherheit zu schützen. Österreich lehnte den Beschluss klar ab, die Niederlande enthielten sich. Mehrere Mitgliedsstaaten signalisierten, dass sie auf Geldspritzen aus Brüssel zur Finanzierung ihrer nationalen Bestandteile des Systems setzen. Die Kommission rechnet mit Kosten in Höhe von insgesamt 500 Millionen Euro. Die Initiative muss nun das EU-Parlament passieren; erste Beratungen sind für Juni 2012 geplant. Berichterstatter im federführenden Innenausschuss ist der britische Konservative Timothy Kirkhope. Großbritannien betreibt bereits seit Jahren eine PNR-Analyse in Eigenregie und drängt auf eine möglichst weite Datenerfassung. Die Fraktionen der Liberalen, der Grünen und der Linken haben sich genauso wie der europäische Datenschutzbeauftragte Peter Hustinx und Datenschützer der Mitgliedsstaaten entschieden gegen das Vorhaben gestellt.

Der Bundesdatenschutzbeauftragte Peter Schaar warnt, dass die von den Innenministern beschlossene „anlasslose mehrjährige Vorratsspeicherung von Daten unverdächtiger Flugpassagiere ein weiterer großer Schritt zur lückenlosen Überwachung alltäglichen Verhaltens wäre". Genau dagegen habe das Bundesverfassungsgericht in seinem Urteil zur Vorratsdatenspeicherung erhebliche Bedenken vorgebracht. Schaar kritisierte auch, dass die Informationen in bedenklicher Art verwendet werden sollen. Alle Fluggäste könnten auf Grundlage der Daten einer „Gefahrenanalyse" unterzogen werden, die einer Rasterfahndung sehr nahe komme (Krempl www.heise.de 27.04.2012; Winter SZ 27.04.2012, 1; SZ 19./20.05.2012, 8).

Europa

INDECT - Sicherheitsforschung auf dem Prüfstand

Die Kommission der Europäischen Union (EU) hatte ein 15-Millionen-Vorhaben zur Verbesserung der öffentlichen Sicherheit durch intelligente Datenverarbeitung ausgeschrieben. Ein Konsortium rund um die Universität Krakau erhielt den Forschungsauftrag im Kontext des 7. Forschungsrahmenprogramms des EU und ist damit eines von 60 geförderten EU-Projekten im Bereich der Sicherheitsforschung. Die Entwicklung im Projekt Indect startete 2009 und wird voraussichtlich bis Ende 2013 andauern. Indect steht für „Intelligent information system supporting observation, searching and detection for security of citizens in urban environment", in deutsch also „Intelligentes Informationssystem zur Unterstützung von Überwachung, Suche und Erfassung für die Sicherheit von Bürgern in städtischer Umgebung". Die Entwickler wollen in dem Projekt digitale Kameras, Gesichts- und Verhaltenserkennung, Spionagetools für PC und Internet und ähnliche moderne Formen der Datenverarbeitung vernetzen und zur Detektion von Risiken nutzen.

Indect soll helfen, Gewalttaten oder Katastrophen frühzeitig zu erkennen und Leben zu retten, indem es die Polizeiarbeit computergestützt automatisiert. Waldbrände oder andere Natur- und Umweltkatastrophen könnten mit dieser Technik schneller entdeckt werden. Auf Großveranstaltungen soll das System Massenpanik erkennen, an Badestränden und Seen unterstütze es Lebensretter; die Technik könne sogar in der Nacht oder im Winter Ertrinkende auffinden und Retter informieren. Die Verbrechensbekämpfung soll eine weitere wichtige Aufgabe von Indect sein. Statt eines Beamten, der bei einer Straftat einschreitet, soll die Technik diese erkennen, bevor sie statt-

findet, indem sie abnormales, gewalttätiges oder kriminelles Verhalten feststellt. Um aber solche Straftaten zu erahnen, ist in dem Projekt tendenziell eine Totalkontrolle aller BürgerInnen nötig. Verschiedene Überwachungsmittel wie Kameras, Drohnenbeobachtung, Gesichtserkennung und Bildanalysen sollen zusammengeschaltet werden, ebenso wie über das Netz „Webseiten, Diskussionsforen, Usenet-Gruppen, Dateiserver, Netzwerke und individuelle Computersysteme", also z. B. P2P-Netzwerke. U. a. wird versucht, „Computerlinguistik so weiterzuentwickeln, dass die Suchroutinen in der Lage sind, Beziehungen zwischen Personen sowie den Kontext einer Unterhaltung, z. B. in Chats, bei der Interpretation der Sprache mit einzubeziehen".

Im Projekt Indect untersuchen die Forschenden, wie sie bestehende Überwachungssysteme so miteinander verbinden können, dass diese die Polizei auf intelligente Weise bei der Verbrechensbekämpfung und Prävention unterstützen. Beispielhaft sind die folgenden Techniken, an denen die EntwicklerInnen forschen:

- **Fliegende Kameras**
  Mit Kameras ausgestattet sollen sie in Zukunft für Sicherheit in Städten sorgen und Streifenpolizisten unterstützen oder sogar ersetzen. Sie liefern genaue Bilder, identifizieren und verfolgen Personen und können hierzu miteinander kommunizieren.
- **Spionage-Software**
  Spionagesoftware soll auf den Rechnern von Verdächtigen deren gesamtes Nutzungsverhalten überwachen. Ob gemäß Indect dieser EU-Trojaner flächendeckend oder nur bei Verdacht eingesetzt werden soll, ist nicht bekannt.
- **Verhaltensanalyse**
  Indect soll erkennen, wenn sich Personen im Alltag abnormal verhalten. Wer einen Koffer am Flughafen stehen lässt, kann ein Attentäter sein. Verdächtig ist man für Indect auch, wenn man sich ungewöhnlich bewegt oder einen Gegenstand in der Hand hält.
- **Personentracking**
  Während eine Überwachungskamera aufzeichnet, dass ein Autofahrer sich verkehrswidrig verhält, checkt das Team von Indect im Hintergrund, ob Infos über den Fahrzeughalter oder das Auto vorliegen und verfolgt dessen Fahrt – beispielsweise mit einer Drohne.

Folgende Arbeitsergebnisse wurden in Aussicht gestellt:
- Testinstallation von Überwachungssystemen zur Gefahrenerkennung in großstädtischen Bereichen,
- Geräte zur mobilen Objektverfolgung,
- Erstellung einer Suchmaschine mit der Möglichkeit einer semantischen Suche in Dokumenten, basierend auf Wasserzeichen,
- System zur Verfolgung krimineller Aktivität und Gefahrerkennung im Internet,
- Sicherstellung von Datensicherheit und Schutz der Privatsphäre durch den Einsatz von Wasserzeichentechnologie und kryptografische Algorithmen.

Beteiligt sind an dem Projekt folgende Hochschul-Einrichtungen:
- Berg- und Hüttenakademie Krakau (Polen),
- Technische Universität Danzig (Polen), Koordinator Andrzej Dziech,
- Universität Carlos III Madrid (Spanien),
- Technische Universität Sofia (Bulgarien),
- Bergische Universität Wuppertal (Deutschland),
- Universität York (Großbritannien),
- Technische Universität Ostrava (Tschechien).
- Fachhochschule Technikum Wien (Österreich)

Beteiligt sind weiterhin Firmen, darunter die deutschen Unternehmen:
- Innotec Data GmbH (Überwachungskameras, Drohnen),
- X-Art ProDivision,
- PSA AG (Psi Transcom, technische Plattform zur Verknüpfung der Informationsquellen).

Die Grundidee

Jede Person wird bei Indect – ähnlich der aktuell ausgesetzten Vorratsdatenspeicherung – unter Generalverdacht gestellt. Die in Aussicht genommenen Überwachungs- und Auswertungsmethoden sind aber deutlich weitreichender als bei der Speicherung der Telekommunikationsverkehrsdaten. Indect setzt voraus, dass Telefonate protokolliert werden und EU-Trojaner Verdächtige beim Mailen oder Chatten überwachen. Indect soll das Kaufverhalten der Betroffenen analysieren, indem es beispielsweise die Kreditkartenzahlungen beobachtet. Auch in der Familie oder im Freundeskreis wird nach Verdächtigen gefahndet. Jeder Bekannte mit Vorstrafenregister könnte so als Gefahr eingestuft werden. Die Maßnahmen sollen die Polizeiarbeit erleichtern.

Ein Fallbeispiel: Sucht z. B. jemand auf einem Parkplatz nach seinem Auto, läuft dann irritiert einmal um den Wagen herum und benötigt dann noch verhältnismäßig viel Zeit, bis er den Schlüssel findet, steigt in den Wagen ein und fährt davon, so wird das von Kameras registrierte Verhalten bei einer Musterauswertung als auffällig eingestuft werden. Die Folge kann dann sein, dass die Gesichtserkennung aktiviert und die Aufnahmen mit einem Bilderpool der Polizei oder Fotos aus sozialen Netzwerken abgeglichen werden. Wird derart die Identität festgestellt, so werden alle zur Person gespeicherten und verfügbaren Informationen abgefragt, ebenso wie die Daten zum Fahrzeug und dessen Halter. Ist das Auto nicht auf den Namen der identifizierten Person angemeldet, kann eine fliegende Drohne das Fahrzeug verfolgen und gegebenenfalls eine Polizeisteife anfordern, die den Fahrer überprüft.

Das Szenario macht die Problematik der Indect-Grundannahmen deutlich: Ab wann ist man verdächtig? Was ist abnormales Verhalten, das eine genaue Observierung und Verfolgung rechtfertigt? Im obigen Beispiel könnte es sich in der Tat um ein Verbrechen handeln, wenn die erfasste Person zuvor den Schlüssel des Fahrzeughalters entwendet hat und nun das Auto klaut. Es könnte sich aber auch um den Freund der Fahrzeughalterin handeln, der sich das Auto geliehen hat und sich Sorgen macht, ob er jemanden beim Einparken touchiert und eine Delle in die Karosserie gefahren hat.

Was „abnormes" Verhalten ist, soll z. B. auch hinsichtlich von Vorgängen in Fußballstadien festgestellt werden. Hooligans sollen im Fanblock an-

hand ihrer Gesänge identifiziert werden. Massenpaniken sollen anhand von Zuschauerbewegungen frühzeitig erkannt werden. Es wird das Ziel verfolgt, abnormales Verhalten von Menschenmassen in Stadien oder auf Musikfestivals zu erkennen, die Bewegungsmuster bei Paniken sind schon gut erforscht. Die Verhaltensweisen im Alltag sind dagegen sehr viel komplexer und selten eindeutig. Eine Technik dürfte kaum in der Lage sein, zwischen einer harmlosen Schulhofrauferei und dem Beginn einer brutalen Schlägerei so schnell zu unterscheiden, dass – aber nur dann – im Notfall jemand zu Hilfe eilen und einschreiten kann Die Indect-Projektteilnehmer nennen ungern Beispiele, wann ein Verhalten abnormal ist und wann nicht.

Auf Anfrage des Europäischen Parlaments wurde etwas deutlicher, was sich Polizisten unter „abnormal" vorstellen: Verdächtig sei jemand, der rennt oder lärmt, im öffentlichen Nahverkehr auf dem Fußboden sitzt oder dort sein Gepäck vergisst. Indect solle aktiv werden, wenn Personen herumlungern oder in der Fußgängerzone gegen den Strom laufen. Die schwammig definierten Tätigkeiten können lapidar sein, die jeden Menschen irgendwann einmal gefährlich erscheinen lassen und normale BürgerInnen unter Generalverdacht stellen.

Die Frage, wann ein Mensch sich abnormal verhält und wann nicht, ist nicht das einzige Rätsel, das Indect aufwirft. Die Initiatoren um die federführende Technische Universität Krakau präsentieren sich auf der Internetseite http://www.indect-project.eu scheinbar offen und stellen oberflächliche Infos ins Netz. Doch konkrete journalistische Anfragen an die beteiligten Firmen zum Stand der Entwicklung blieben immer wieder unbeantwortet.

Reaktionen

Nachdem die Zielsetzung und der methodische Ansatz von Indect bekannt und öffentlich kritisiert wurde, distanzierte sich das deutsche Bundeskriminalamt (BKA) ausdrücklich von diesem Projekt. Der umfassende Überwachungsgedanke von Indect sei mit dem vom BKA verfolgten rechtsstaatlichen Ansatz nicht vereinbar. Die staatlichen Datenschutzbeauftragten wurden erst durch Medienberichte auf das Forschungsprojekt aufmerksam. Auch Mitglieder des Europäischen Parlaments (EP) bemängelten die fehlende Kommunikation: Sie forderten Einblicke in eine Bewertung, die von der EU-Kommission über Indect verfasst wurde. Doch die Abgeordneten bekamen die Unterlagen erst nach einjähriger Verzögerung. Darin finden sich widersprüchliche Infos: So stufte die EU-Kommission die Datenschutzbestimmungen von Indect zwar als besorgniserregend ein; dennoch sei das Projekt laut Kommission „ethisch akzeptabel".

Koordinator Dziech reagierte für die Projektpartner, nachdem die Kritik an Indect immer lauter wurde: „Indect ist ein Forschungsprojekt, kein Anwendungsprojekt. Fragen, die mit der Verwertung und den zukünftigen Zwecken zu tun haben, liegen nicht im Rahmen unserer Forschung".

Die fehlende Transparenz ist zwangsläufig Auslöser von Spekulationen: Ein Projektleiter kündigte noch vor dem eigentlichen Projektstart an, dass Indect bei der Fußballeuropameisterschaft 2012 in Polen und der Ukraine getestet werden soll. Auch Meldungen über den Einsatz bei den Olympischen Spielen in London 2012 waren im Umlauf. Zwar dementierten die Forschenden diese Planungen schon im November 2010 ausdrücklich, mussten dies aber nach weiteren Medienberichten erneut per Pressemeldung richtigstellen: Es gebe seitens Indect keine Pläne, die Technik während dieser Turniere einzusetzen. Die mangelnde Offenheit der Indect-Leitung heizte die Spekulationen immer wieder an. Viele Medienleute berichten von unbeantworteten Anfragen.

Merkwürdig ist das Verschwinden zweier Dokumente, die lange Zeit über die Indect-Seite verfügbar waren. In den PDFs ging es darum, welche konkreten Überwachungstechnologien im Rahmen des Forschungsprojekts entwickelt werden sollen. Die Verantwortlichen nannten Serverprobleme als Ursache für das Verschwinden der Dateien. Laut Franz Obermayr, Mitglied des EP, ist der Ethikrat von Indect der Grund für den augenscheinlichen Datenverlust. Dieser Ethikrat besteht v. a. aus Mitgliedern, die in Indect involviert sind, also Polizisten und Vertretenden der forschenden Firmen – also befangenen Personen mit eigenen wirtschaftlichen Interessen:

- Drew Harris, PSNI Assistant Chief, Police,
- Dobroslaw Kot, External Doctor of Philosophy,
- Emil Plywaczewski, External Academia, Professor of Law,
- Andreas Pongartz, X-Art Industry, Head of the company,
- Tom Sorell, PSNI Human Rights Lawyer,
- Zulema Rosborough, PSNI Police Officer,
- Mariusz Ziolko, AGH Researcher security related technologies.

Die Bezeichnung „Ethikrat" ist irreführend. Er soll nicht das Projekt kritisch hinterfragen und die Privatsphäre der BürgerInnen schützen, sondern alle Dokumente vor ihrer Veröffentlichung prüfen, um schlechte Berichterstattungen der Medien zu verhindern. Es handelt sich beim Ethikrat damit eher um eine Zensurinstanz, die dafür sorgen soll, dass das Projekt keiner öffentlichen Kritik ausgesetzt wird.

Der Chaos Computer Clubs sowie die Piratenpartei veröffentlichten die verschwundenen Unterlagen auf ihren Homepages. Mittlerweile sind die Papiere wieder auf der Indect-Seite erhältlich. Die Piraten stemmen sich massiv gegen Indect, etwa über die Seite stopp-indect.info. Nachdem viele PolitikerInnen den Ethikrat und seine Zusammenstellung kritisierten, wurden die Piraten sogar von Indect eingeladen, mit einem Sitz der Runde beizuwohnen, was diese jedoch ablehnten. Stephan Urbach von der Piratenpartei erläuterte: „Ein einziger Platz kann nicht viel verhindern. Sollte Indect dann doch kommen, wäre es legitimiert von den Piraten." Dies wolle sich die junge Partei nicht vorhalten lassen.

Am 12.04.2012 ordnete das polnische Innenministerium nach Rücksprache mit der an INDECT beteiligten Polizei den Ausstieg aus dem Projekt an mit der Begründung, die Polizei verfüge über „ausreichende Mittel zur Abwehr von Gefahren". Tatsächlicher Hintergrund des Ausstiegs war aber wohl eher die

auch in Polen zunehmende öffentliche Kritik an dem Projekt. Der Vorgang veranlasste den Bundestagsabgeordneten der Linken Andrej Hunko, den Rückzug auch der deutschen Teilnehmer aus dem Projekt zu fordern.

Nicht wenige ExpertInnen zweifeln an der Realisierbarkeit der vollmundigen Versprechen der Indect-Projektpartner. So sei es fragwürdig, dass die koordinierende Technische Universität Krakau wirklich über die Qualitäten verfügt, ein Konsortium aus 18 Projektpartnern effektiv zu managen und das disparate Patchwork technischer Teilprojekte zu einem integrierten urbanen Überwachungssystem zusammenzuführen. Es dürfte plausibler sein, dass einzelne Module im Verlauf des Projektes zur Praxistauglichkeit heranreifen und letztlich isoliert ihren Weg in den Alltag suchen. Doch selbst dann bleibt die Frage, welche Chancen für eine erfolgreiche Vermarktung bestehen. Das Konsortium mit Universitäten, der nordirischen und bis in jüngste Zeit der polnischen Polizei sowie einigen mittelständischen Unternehmen repräsentiert eher periphere Akteure des sicherheitsindustriellen Komplexes. Dies ist der Grund, weshalb manche Insider behaupten, dass die Genehmigung des Projektes mehr dem europäischen Proporzdenken geschuldet sei als einem überzeugendem Forschungsplan.

Sicherheitsforschung generell

Indect eignet sich ideal als Projektionsfläche der Ängste vor der „Forschung für den Überwachungsstaat". Zwar ist INDECT mit seinem 15-Millionen-Euro-Budget das teuerste Projekt in der Förderlinie „Sicherheit der Bürger". Aber diese ist nur eine – zudem kleinere – unter insgesamt sieben Förderlinien. Indect ist nur eines von mehr als 130 Projekten, die seit 2007 im Rahmen des Europäischen Sicherheitsforschungsprogramms bewilligt wurden. Von A wie ADABT („Automatic detection of abnormal behaviour and threats in crowded spaces") bis W wie WIMA2S („Wide maritime area airborne surveillance") zielen zahlreiche dieser Projekte auf die Entwicklung und Perfektionierung von Überwachungssystemen - und einige von ihnen mit absehbar größerem Erfolg als der mutmaßliche „Bevölkerungsscanner".

Im Rahmen des 1,4 Milliarden Euro schweren Sicherheitsforschungsprogramms der EU gibt es mehrere Projekte, die teurer sind, aber für weniger Furore sorgen, da sie die BürgerInnen nur mittelbar betreffen. Sie sollen beispielsweise zur Grenzüberwachung verwendet werden. Das größte Projekt ist Perseus unter der Leitung des spanischen Technologiekonzerns Indra, das über ein Budget von 44 Millionen Euro verfügt, wovon über die Hälfte aus EU-Geldern stammt. Den Rest steuern die beteiligten Unternehmen selbst bei. Das Gesamtvolumen für Überwachungstechnologien schätzen ExpertInnen auf ca. 100 Mrd. Euro, mit jährlichen Wachstumsraten von ca. 5%. Referenzprojekte werden deshalb gefördert, so die Broschüre „Zukunftsmarkt Zivile Sicherheit" des FDP-geführten Bundeswirtschaftsministeriums. Exporte deutscher Firmen sollten politisch flankiert, die Ausfuhrkontrolle entschlackt und beschleunigt werden. Als Zielmärkte gelten bzw. galten neben Fernost Osteuropa, Nordafrika (bis zum arabischen Frühling) und die Golfstaaten.

Ein Beispiel für den Realeinsatz eines Forschungsprojektes ist ein heliumgefüllter Ballon, der mit hochauflösender Kamera 2011 das Sommerfest des Südwestrundfunks (SWR) mit 20.000 Teilnehmenden beobachtete. Mit dem Motto „Sie feiern und wir passen auf!" warb das Fraunhofer Institut für Optronik, Systemtechnik und Bildauswertung (IOSB), deren Forschende das Gerät entwickelt hatten, für diese Aktion. Sie sollte demonstrieren, wie weit Überwachungstechnik entwickelt ist und in welchen Alltagssituationen sie eingesetzt werden kann. Nach öffentlicher Kritik an der eigenartigen forschenden Überwachung, erklärte das Institut eilig, weder die Gesichtserkennung einzusetzen noch die Daten zu speichern. Die Drohne, die als Teil eines militärischen Systems für Sicherheit sorgen soll, zeigt, wie weit die Forschung auf diesem Gebiet mittlerweile ist, wie militärische Entwicklungen in unseren Alltag einfließen und in Zukunft unser Leben beeinflussen. Das Fraunhofer-System hat den Namen AMFIS (Aufklärung mit mobilen und ortsfesten Sensoren im Verbund).

Ergebnisse aus der Sicherheitsforschung dürfen nicht direkt vom Staat eingesetzt werden. Sie müssen zuvor vom Gesetzgeber legitimiert werden. Es ist schwer einzuschätzen, wie realistisch es ist, dass die entwickelten Überwachungsinstrumente umgesetzt werden. Selbst die Indect-Macher äußerten sich dahingehend, dass es keine Garantie für den Einsatz der Technik gebe. Indect-Forscher Jan Derkacz meinte: „Von uns wird nicht erwartet, dass wir am Ende ein fertiges Produkt liefern." Doch bekräftigte er, dass Indect sehr realitätsnah entwickelt wurde und daher gute Aussichten auf eine Verwendung habe. Auch Pirat Urbach glaubt, dass Indect – trotz aller datenschutzrechtlichen Bedenken – nicht zu stoppen sei: „Indect wird so formuliert sein, dass es verfassungskonform ist." Auch die Vorratsdatenspeicherung habe nicht generell gegen das Grundgesetz verstoßen. Alexander Alvaro, EP-Mitglied für die Liberalen, beruhigte dem gegenüber: „Es gibt mindestens drei Grundgesetz-Artikel, die gegen den Einsatz von Indect sprechen." Er bezweifelt, dass Indect vom Europäischen Parlament legitimiert wird, es bestehe lediglich die Gefahr, dass einzelne Teile gewissermaßen ins Polizeiwerkzeug eingeschmuggelt werden.

In einem aktuellen Gesetzentwurf vom Dezember 2011 stellt sich für Deutschland die Bundesregierung zumindest auf den Einsatz von Drohnen ein: Die Regierung will erlauben, dass unbemannte Luftfahrtsysteme fliegen können, ohne Flugzeugen in die Quere zu kommen. Im Gesetzentwurf heißt es zwar auch, dass die technischen Voraussetzungen für einen reibungslosen Einsatz noch nicht gegeben seien. Doch sobald diese erfüllt sind, könne eine entsprechende Verkehrszulassung und Registrierung kommen. Dass Drohnen ein bestimmtes Gebiet problemlos überwachen können, hat der Einsatz bei dem SWR-Sommerfest gezeigt.

Reaktion der Datenschutzbeauftragten

Die fragwürdige Sicherheitsforschung hat die Konferenz der Datenschutz-

beauftragten des Bundes und der Länder auf ihrer Sitzung am 21./22. März 2012 in Potsdam unter dem Titel „Öffentlich geförderte Forschungsprojekte zur Entdeckung abweichenden Verhaltens im öffentlichen Raum – nicht ohne Datenschutz“ zu folgender Entschließung veranlasst:

„Mit erheblichen öffentlichen Mitteln werden derzeit zahlreiche Forschungsprojekte finanziert, die darauf abzielen, mit Hilfe modernster Technik – insbesondere der Videoüberwachung und dem Instrument der Mustererkennung – menschliche Verhaltensweisen zu analysieren. Dadurch sollen in öffentlich zugänglichen Bereichen mit hohem Sicherheitsbedarf „potentielle Gefährder“ frühzeitig entdeckt werden. Zu derartigen Forschungsvorhaben zählen beispielsweise das Projekt „INDECT“ (Intelligentes Informationssystem zur Überwachung, Suche und Detektion für die Sicherheit der Bürger in urbaner Umgebung), das von der Europäischen Union gefördert wird, oder in Deutschland Projekte wie ADIS (Automatisierte Detektion interventionsbedürftiger Situationen durch Klassifizierung visueller Muster), CamInSens (Verteilte, vernetzte Kamerasysteme zur in-situ-Erkennung personeninduzierter Gefahrensituationen) oder die Gesichtserkennung in Fußballstadien.

Bei der Mustererkennung soll auf Basis von Video- oder anderen Aufzeichnungen, die mit Daten aus anderen Informationsquellen kombiniert werden, das Verhalten aller erfassten Personen computerunterstützt ausgewertet werden. Menschen, deren Verhalten als ungewöhnlich eingestuft wird, können so in Verdacht geraten, zukünftig eine Straftat zu begehen. Gerade bei der Mustererkennung von menschlichem Verhalten besteht daher die große Gefahr, dass die präventive Analyse einen Anpassungsdruck erzeugt, der die Persönlichkeitsrechte der betroffenen Bürgerinnen und Bürger verletzen würde.

Insoweit ist generell die Frage aufzuwerfen, inwieweit die grundrechtliche Zulässigkeit des Einsatzes der zu erforschenden Überwachungstechnik hinreichend untersucht wird. Bei Projekten, bei denen öffentliche Stellen des Bundes und der Länder beteiligt sind, sollten jeweils die zuständigen Datenschutzbehörden frühzeitig über das Projektvorhaben informiert und ihnen Gelegenheit zur Stellungnahme eingeräumt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an alle öffentlichen Stellen von Bund und Ländern, aber auch an die der Europäischen Union, die solche Projekte in Auftrag geben oder Fördermittel hierfür zur Verfügung stellen, bereits bei der Ausschreibung oder Prüfung der Förderfähigkeit derartiger Vorhaben rechtliche und technisch-organisatorische Fragen des Datenschutzes in ihre Entscheidung mit einzubeziehen. Nur so kann verhindert werden, dass Vorhaben öffentlich gefördert werden, die gegen Datenschutzvorschriften verstoßen.“

(BT-Drs. 17/3940 v. 25.11.2010, Forschung am EU-Projekt INDECT; Disput zwischen Johnigk/Nothdurft, FIfF, mit Derkacz, INDECT, in: FIfF-Kommunikation 3/2011, 50 ff. m.w.N.; Behrens SZ 01.12.2011, 20; Hoferer www.focus.de 16.03.2012; PE Hunko vom 18.04.2012; de.wikipedia.org Stichwort „INDECT“; zum Thema Sicherheitsforschung generell Töpfer, Die großen Brüder von INDECT, Telepolis, www.heise.de 28.11.2011).

Frankreich

Zentrale Fingerabdruckdatei beschlossen

Die Regierungsparteien in Frankreich haben zur Bekämpfung von Identitätsdiebstahl am 06.03.2012 mit ihrer Mehrheit ein „Gesetz zum Schutz der Identität“ (Loi relative à la protection de l‘identité) verabschiedet. Es sieht die Speicherung von Fingerabdrücken in Personalausweisen (Carte d‘identité) und Reisepässen vor. Anders als in Deutschland sollen zudem die persönlichen und biometrischen Daten dauerhaft in einem Zentralregister vorgehalten werden, auf das unter anderem die Strafverfolgungsbehörden zugreifen können. Die Oppositionsparteien kritisierten das Gesetz scharf. Der sozialistische Abgeordnete Jean-Jacques Urvoas meinte: „In diesem Text geht es um die Erstellung einer Datei von in unserem Land bislang unerreichtem Umfang, denn sie wird die gesamte Bevölkerung betreffen! Keine andere Demokratie hat es gewagt, diese Grenze zu überschreiten.“ Marc Dolez von der demokratischen Linken (GDR) warnte, das Gesetz werde „unser Land dem Risiko von Prozessen vor dem europäischen Menschenrechtsgerichtshof aussetzen, und das Risiko ist groß, dass Frankreich dort verurteilt wird.“ Für die Regierung begründete Pascal Brindeau das Vorhaben: „Durch die vorgesehene Zentraldatei will das Gesetz eine echte Plage beenden, die jedes Jahr mehr als 200.000 Opfer fordert.“ Wie bei jedem Sicherheitsthema müsse man Rechte und Freiheiten mit den Bedürfnissen der Strafverfolgungsbehörden in Einklang bringen. Diese benötigten Werkzeuge und Daten, um ihre Aufgaben effizient zu erfüllen. Gemäß Presseberichten will die Sozialistische Partei gegen das Identitätsgesetz vor dem französischen Verfassungsgerichtshof klagen (www.heise.de 08.03.2012).

Frankreich

Ikea soll MitarbeiterInnen und KundInnen bespitzelt haben

Im Umgang mit einigen seiner KundInnen und MitarbeiterInnen griff der französische Ableger des schwedischen Ikea-Konzerns offenbar zu rabiaten Methoden. Ikea soll über Jahre hinweg den Alltag mancher MitarbeiterInnen und KundInnen ausgeforscht haben. Gemäß Medienberichten sollen sich die Möbelhaus-Spione unter anderem für persönliche Bankkonten, Führerscheine und Autopapiere interessiert haben. Datenbeschaffungen erfolgten aus der zentralen Polizeikartei, aus der Kfz-Zulassungsstelle oder aus dem Führerscheinregister. Selbst bei Gerichtsakten laufender Untersuchungen soll sich die Firma bedient haben. Informationen über die Liebesbeziehungen von Mitarbeitenden sollen über Jahre mit illegalen Methoden an Ikea gelangt sein. Bewerbende wurden danach vor ihrer Anstellung über-

prüft, ebenso Gewerkschafter und KundInnen im Fall einer geschäftlichen Auseinandersetzung. Ikea hat in Frankreich 29 Standorte und macht mehr als zwei Milliarden Euro Umsatz.

Der Konzern hat sich nach Bekanntwerden der Vorwürfe von jeglichen Spionage-Praktiken distanziert. „Wir nehmen die Veröffentlichung dieser Vorwürfe sehr ernst“, versicherte die Unternehmensführung in Frankreich. „Der Respekt vor dem Privatleben zählt zu den wichtigsten Werten unserer Gruppe.“ Die Zeitung „Canard enchaîné“ berichtete, dass das Unternehmen zum Ausspionieren seiner „Zielpersonen“ die Dienste von privaten Sicherheitsdienstleistern, u. a. von der Firma Sureté International, in Anspruch nahm. E-Mails, die auch auf der Seite des Internetdienstes Mediapart veröffentlicht wurden, zeigen, dass Ikea seit Dezember 2003 mit dem Detektivbüro systematisch den heimlichen Zugriff verabredete. Für „80 Euro die Konsultation“ versprach danach die Sicherheitsfirma Informationen aus dem staatlichen Zentralregister „Stic“: Das „System für die Behandlung festgestellter Vergehen“ ist ein elektronischer Dienst unter dem Dach des Innenministeriums, der Hinweise im Zusammenhang mit Straftaten – die Identität von Tätern, Diebesgut und Opfern – sammelt. Der Zugang zu dem System, aus dem monatlich Daten zu rund 15.000 Personen abgefragt werden, sollte eigentlich auf Polizei, Gendarmerie und Justiz beschränkt sein.

Spitzel in Diensten des Möbelhauses hatten aber offenbar Zugriff auf die Daten des Registers. Die Anfragen der Ikea-Bosse waren demnach immens und präzise: „Vertraulich: (…) Ich brauche Informationen über sein Strafregister und seinen Lebensstil“, beginnt eine dokumentierte Anfrage vom Chef der Ikea-Abteilung für Sicherheit an eine Detektei. Er führt weiter aus, was ihn interessiert: „In der Tat fährt unser Freund in einem ‚neuen‘ BMW-Coupé, und der junge Mann könnte einen Lebenswandel führen, weit über seinem Einkommen (Kleidung, Ausgehen…). Das Autokennzeichen teile ich Ihnen so schnell wie möglich mit (…).“ Aus weiteren E-Mails an Ikea-Verantwortliche Wochen später geht hervor, dass auch die Konten des Betroffenen bei der Post und einer Bank ausgeforscht werden sollten. Ikea interessierte sich auch für intime Details von „Zielpersonen“. So erhielt im August 2003 eine Detektei den Auftrag, für die Ikea-Filiale in Toulouse Hintergrundmaterial über eine Mitarbeiterin zu beschaffen, die dort sechs Jahre beschäftigt war. Das Motiv: „Ihr Lebenspartner könnte ein ‚Zigeuner‘ sein, der als gefährlich gilt.“ Wie die ausgespähte Mitarbeiterin berichtete, schellten die Alarmglocken, wenn Roma die Hallen betraten: „Es gab einen Code – ‚Madame Marty wird im Laden verlangt‘“, schilderte die Frau Ansagen per Lautsprecher. „Dann erschienen alle Verantwortlichen und hefteten sich den Zigeunern an die Fersen: Sie waren ‚persona non grata‘“ – unerwünscht.

Führungspersonal vom Ikea-Standort Paris Nord 2 verschaffte sich offenbar auch Zugang zu Gerichtsakten aus einem laufenden Verfahren, das gegen Gewerkschafter des Unternehmens angestrengt wurde. Gemäß in der Presse veröffentlichten E-Mails konnte sich der Ikea-Funktionär nicht nur Hinweise zur Strategie der betrauten Untersuchungsrichterin beschaffen, sondern über Kontakte bei der Kripo auch die Verhörprotokolle der Ikea-Mitarbeiter einsehen. Dass er illegal handelte, war ihm offenbar voll bewusst: „Offiziell bin ich natürlich nicht gehalten, Zugang zu den Akten zu haben“, schließt der Bericht an seine Vorgesetzten. „Ich kann daher keine Namen und Daten nennen.“ „Wir hatten unseren Verdacht“, sagte Gewerkschaftsvertreter Salvatore Rinaldo. Zwar habe es keine Beweise gegeben, allerdings habe jemand davon berichtet, dass alles, was die MitarbeiterInnen taten, auf USB-Sticks gespeichert werden musste. Ein betroffener Mitarbeiter habe sich jedoch geweigert und sei daraufhin entlassen worden.

Spionage durch Firmen scheint in Frankreich kein Einzelfall zu sein: Der Euro Disney Park bei Paris und drei ehemalige Polizisten müssen sich ab Herbst 2012 wegen der mutmaßlichen Bespitzelung von mehreren tausend Stellenbewerbenden vor Gericht verantworten. Wie ein Gerichtssprecher mitteilte, soll der Prozess im September im Städtchen Meaux östlich von Paris beginnen. Das Unternehmen soll sich ähnlich wie Ikea Frankreich illegal personenbezogene Daten beschafft haben. Auch für den Möbelkonzern könnte die Affäre rechtliche Konsequenzen haben. Die Gewerkschaft Force Ouvrière hat Anzeige erstattet, die zuständigen Behörden in Versailles haben Vorermittlungen eingeleitet. Auch manche der ausgespähten ehemaligen KundInnen und MitarbeiterInnen überlegen, Ikea zu verklagen. Das wird jedoch dadurch erschwert, dass die in den E-Mails genannten privaten Sicherheitsfirmen inzwischen abgewickelt worden sind. Ikeas PR-Chef versprach, „alles zu tun“, um Licht in die Affäre zu bringen - auch unter Einschaltung einer firmenfremden Kanzlei. Auch das Innenministerium gelobte, im Falle einer Klage nachzuprüfen, ob staatliche Informationsquellen illegal benutzt wurden (Simons www.spiegel.de 02.03.2012; www.welt.de 29.02.2012).

Frankreich

Rassismusvorwurf gegen Google wegen „Autocomplet“-Suchangebot

Vier französische Menschenrechtsorganisationen, darunter SOS Racisme, haben dem französischen Ableger des US-Konzerns Google „latenten Antisemitismus“ vorgeworfen und diesen deswegen angezeigt. Google muss sich nun vor einem Gericht in Paris wegen seiner Suchfunktion „Autocomplet“ verantworten. Der Vorwurf: Menschen würden nach ethnischen Kriterien erfasst und kategorisiert, was in der laizistischen Republik Frankreich verboten ist. Bei der Suche nach Prominenten taucht oft als erste Option der Begriff „juif“ (Jude) auf, in vielen Fällen zudem fehlerhaft. Wer z. B. den Nachnamen des neuen französischen Präsidenten „Hollande“ in das Suchfeld der französischen Seite eingibt, findet als erste Ergänzungsmöglichkeit „juif“. Das gleiche galt bis zur Wahl am 06.05.2012 auch für seinen Vorgänger Nicolas Sarkozy. Konzernchefs und VertreterInnen des Showbusiness werden ebenfalls mit der Ergänzung verse-

hen. Patrick Kluman, Anwalt von SOS Racisme, sieht darin die Gefahr, dass antisemitische Ressentiments geschürt werden.

Google streitet jede eigene „ideologische Verantwortung" ab. Es handele sich vielmehr um eine Frage des Algorithmus. Google beeinflusse die „Autocomplete"-Funktion nicht gezielt. Sie diene vielmehr dazu, eine schnellere Suche zu ermöglichen. Das mathematische Prinzip dahinter sei so ausgerichtet, dass die Begriffe, die von den Nutzenden am meisten eingegeben werden, automatisch an oberster Stelle erschienen. Wenn also die Bezeichnung „Jude" als Option auftauche, sage das nichts über die Religionszugehörigkeit der gesuchten Person, sondern vielmehr etwas über das Suchverhalten der französischen Internetnutzenden. Dies bestätigt Jonathan Hayon, Vorsitzender des klagenden jüdischen Studentenverbands UEJF, der meint, „dass es eine französische Obsession ist herauszufinden, ob dieser oder jener in der Medien- oder Finanzwelt jüdisch ist". Gemäß einer Umfrage aus dem Jahr 2011 glaubten 30% der FranzösInnen, Juden hätten in diesen Bereichen mehr Einfluss als andere. Der Begriff „Jude" muss nicht per se abwertend gemeint sein. Es könne auch Juden geben, die aus Interesse nachschauen, welche bekannten Persönlichkeiten ihrer Religion angehören. Dazu gehören z. B. auch die Google-Gründer.

2009 verurteilte die Justiz den französischen Ableger von Google, weil die halbautomatische Suchvervollständigung hinter den Firmennamen des Energieanbieters Direct Energie das Wort „Nepp" setzte. Das betroffene Unternehmen klagte und gewann gegen Google, das den Algorithmus ändern musste. Google tut derweil auch im konkreten Fall so, als sei es neutral. Das steht jedoch in Widerspruch zu einer Mitteilung, dass der Algorithmus auf „einer Reihe von Faktoren, wie z. B. der Popularität" basiere. Die Faktoren wären demnach menschengemacht und keinem höheren mathematischen Objektivitätsprinzip unterworfen. Google könnte einen entsprechenden Filter schalten, um unerwünschte Assoziationen zu tilgen. Gemäß den klagenden Menschenrechtsorganisationen geht es ihnen um den Schutz der Persönlichkeitsrechte. In Zeiten von „Shitstorms", in denen Einzelne in einen Strudel von Verleumdungen geraten könnten, seien schützende Filter angebracht. Algorithmen ließen sich manipulieren. Google beharrt dagegen auf seiner Haltung und pocht auf die Freiheit des Internets (Kläsgen SZ 12./13.05.2012, 27).

Großbritannien

Regierung plant massive Ausweitung der Verkehrdatenüberwachung

Die britische liberal-konservative Regierung will das bislang umfassendste Gesetz zur Überwachung des Kommunikationsverhaltens der BürgerInnen in einem EU-Mitgliedsstaat einführen und es ermöglichen, dass die Behörden Informationen über E-Mails, angesurfte Webseiten, Anrufe und SMS erhalten. Die Überwachung soll durch das Government Communications Headquarters (GCHQ) vorgenommen werden. Polizei, Geheimdienste und andere staatliche Stellen sollen ohne richterliche Genehmigung in Echtzeit auf die Daten zugreifen können. Schon seit 2009 müssen Telekommunikationsunternehmen 12 Monate lang speichern, wer mit wem wann wie lange und wo telefoniert hat. In Zukunft soll auch erfasst werden, was Menschen in Netzwerken wie Facebook tun, mit wem sie über Internettelefondienste wie Skype sprechen und welche Websites sie besuchen. Ein Sprecher des Innenministeriums erläuterte: „Es ist lebensnotwendig, dass Polizei und Sicherheitsdienste unter bestimmten Umständen Zugriff auf Kommunikationsdaten erhalten, um schwere Verbrechen und Fälle von Terrorismus zu untersuchen und die Öffentlichkeit zu schützen." Aus den Daten ließen sich aussagekräftige Kommunikationsprofile von einzelnen BürgerInnen erstellen. Nick Pickles, Direktor der Aktivistengruppe Big Brother Watch, sprach von einem „bislang beispiellosen Schritt, mit dem Großbritannien die Art von Überwachung einführt, auf die auch Iran und China zurückgreifen". Mit dem Vorstoß geht die aktuelle Regierung über die Speicherpflichten hinaus, die in der umstrittenen EU-Richtlinie zur Vorratsdatenspeicherung vorgesehen sind.

Bereits 2006 hatte die damalige Labour-Regierung ein ähnliches Gesetz geplant. In einer Datenbank sollten Telefonate, SMS, E-Mails und besuchte Webseiten gespeichert und für die Ermittler zugänglich gemacht werden. Schon bald rückte man nach heftigen Debatten von der Idee ab, da Internet-Provider und Mobilfunkanbieter die Machbarkeit bezweifelt und über mögliche hohe Kosten geklagt hatten. Auch die aktuelle Initiative stößt bei den Providern auf wenig Gegenliebe. Die sogenannte „Deep-Packet-Inspection" einzuführen, die versendete Datenpakete auswertet und dabei Sender, Empfänger und Zeitpunkt der Übertragung speichert, sei technisch schwierig und würde zu kaum kalkulierbaren Ausgaben führen. Zudem gebe es „moralische und legale Fragen, ob und wie dies umgesetzt werden sollte", so ein Mitarbeiter eines Internet-Providers. Konservative und Liberale hatten noch 2006 gegen die Überwachungs-Idee der Labour-Regierung protestiert. In ihrem Koalitionsvertrag hatten die Parteien festgelegt, „unnötige Datenspeicherung zu beenden". Entsprechend desillusioniert äußerte sich Shami Chakrabarti von der Gruppe „Liberty": „Man hat das Gefühl, das Imperium schlägt zurück, egal wen man wählt."

Das Gesetz dürfte nicht ohne weiteres die parlamentarischen Hürden nehmen. Als einer der ersten Kritiker aus den eigenen Reihen meldete sich der konservative Abgeordnete David Davis zu Wort, einst Schatten-Innenminister und bekannter Kritiker der Antiterror-Gesetze der damaligen Labour-Regierung: „Das Gesetz betrifft nicht Kriminelle oder Terroristen, es betrifft alle Bürger. Wir brauchen es nicht, um uns zu schützen. Es erweitert unnötigerweise die Möglichkeit des Staates, normale, unschuldige Menschen in großer Zahl auszuschnüffeln. Der Staat sollte diese Möglichkeit einfach nicht haben."

Der Informatiker und Erfinder des World Wide Web, MIT-Professor und

Berater der Regierung Cameron in Internetfragen Tim Berners-Lee meinte, das neue Überwachungsgesetz stelle einen Verstoß gegen die Menschenrechte dar: „Das Maß an Kontrolle, das man über jemanden bekommt, wenn man dessen Internetaktivitäten überwachen kann, ist unglaublich. Man lernt jedes Detail kennen, in gewisser Weise erfährt man mehr intime Dinge über sein Leben als jeder andere, mit dem er spricht, denn oft vertraut man dem Internet und besucht dort Gesundheitswebsites (...), oder Jugendliche suchen eine Website über Homosexualität auf und fragen sich, was mit ihnen los ist und ob sie mit anderen darüber reden sollen.“ Deshalb sei es gefährlich, wenn die Regierung plane, routinemäßig Daten über Internetnutzer zu sammeln. Wenn Daten vorhanden seien, könnten sie auch gestohlen werden. Oder korrupte Beamte oder korruptes Bedienungspersonal könnten damit Mitarbeiter der Regierung oder des Militärs erpressen. Wenn die Regierung schon beabsichtige, solche Daten zu sammeln, dann müsse sie dafür sorgen, dass eine starke und unabhängige Aufsichtsstelle eingerichtet werde. Diese solle dann jede Überwachungsmaßnahme prüfen, um festzustellen, ob der Überwachte tatsächlich eine Bedrohung darstelle und ob die Überwachung Ergebnisse erbracht habe. Bisher habe die Regierung jedoch weder Pläne für eine Aufsicht präsentiert noch habe sie dargelegt, wie die Daten sicher gespeichert werden sollten. Deshalb sei es für ihn das Wichtigste, dass der Entwurf in der aktuellen Fassung gestoppt werde.

Datensicherheit ist ein wichtiges Thema in Großbritannien. In den vergangenen Jahren war es mehrfach zu schweren Datenpannen gekommen. So war etwa ein USB-Stick mit persönlichen Daten von allen Strafgefangenen in englischen und walisischen Gefängnissen verloren gegangen. Einem Lehrerverband kam auf einem Transport eine CD mit Daten von mehr als 11.000 Lehrern abhanden. Auf einem Parkplatz neben einem Pub wurde ein USB-Stick mit Nutzerkennungen und Passwörtern für das E-Government-Portal gefunden (www.sueddeutsche.de 02.04.2012; Pluta www.zeit.de 18.04.2012; Der Spiegel 15/2012, 87).

Polen

Extensive Nutzung der Vorratsdatenspeicherung

Die polnische Bürgerrechtsorganisation Panoptykon Foundation veröffentlichte am 04.04.2012, dass Strafverfolger des Landes im Jahr 2011 fast 1,86 Millionen Verbindungs- und Standortinformationen abgefragt haben; im Jahr davor waren es noch 1,38 Millionen. 2009 griffen die Ermittler gut 1 Million Mal auf die Vorratsdaten zu. Die Daten beruhen gemäß diesen Angaben auf einer Auskunft nach dem polnischen Informationsfreiheitsgesetz vom nationalen Amt für elektronische Kommunikation (UKE). Damit dürfte Polen in der EU-Statistik der Länder, in denen Polizei und Justiz sich am häufigsten die Vorratsdatenspeicherung zunutze machen, weiter eine Spitzenposition einnehmen. Gemäß den aktuellsten Zahlen aus Brüssel hatte sich Tschechien 2008 darauf den Spitzenplatz erobert: 12.744 Abfragen kamen dort vor vier Jahren auf 1 Million Einwohner. In Polen wurde im vergangenen Jahr rund 49.000 Mal pro Million der dort gemeldeten BürgerInnen zugegriffen. Insgesamt 1 Million der Ersuchen 2011 hätten sich auf höchstens einen Monat alte Daten bezogen. Eine Unterscheidung nach Informationstypen und ob die Daten etwa beim Surfen oder Telefonieren angefallen sind, hat das UKE nicht herausgegeben.

In Polen dürfen die Polizei und mehrere andere Behörden verdachtsunabhängig protokollierte Nutzungsdaten nicht nur zur Bekämpfung schwerer Straftaten verwenden, so wie es die EU-Richtlinie vorsieht. Zugriffe sind z. B. auch zur Gefahrenabwehr möglich. Eine Richtergenehmigung brauchen die Sicherheitsbehörden nicht. Die Speicherfrist ist in Polen mit zwei Jahren länger als im EU-Durchschnitt. Panoptykon spricht von einer hohen Zahl missbräuchlicher Nutzungen von Vorratsdaten. Zu den aufsehenerregendsten Fällen gehöre die Bespitzelung von Journalisten durch den Geheimdienst. Jüngst habe zudem ein Warschauer Gericht bestätigt, dass das Büro des Generalstaatsanwalts verdachtsunabhängig gespeicherte Telekommunikationsdaten rechtswidrig eingesetzt hat. Seit über zwei Jahren bemühe man sich um eine Reform der gesetzlichen Grundlagen zur Vorratsdatenspeicherung. Eine für Menschenrechtsfragen zuständige polnische Institution habe bereits Beschwerde beim nationalen Verfassungsgericht eingereicht. In Brüssel bereitet die EU-Kommission derweil eine Überarbeitung der Direktive vor (Krempl www.heise.de 04.04.2012)

Ungarn

EU-Kommission verklagt Ungarn wegen Abhängigkeit der Datenschutzkontrolle

Die EU-Kommission hat den Streit über die Unabhängigkeit der ungarischen Zentralbank beendet. In den Vertragsverletzungsverfahren zur Justiz und zum Datenschutz hingegen klagt sie gemäß einer Mitteilung vom 25.04.2012 gegen Ungarn. Im Streit über das neue Notenbankgesetz hatte die Regierung Orbán in den Gesprächen mit der Kommission eine Reihe von Zugeständnissen gemacht, die umgehend im ungarischen Parlament verabschiedet werden sollen.

Dass die Kommission in den beiden anderen Verfahren gegen Ungarn klagen würde, war schon zuvor in Brüssel bekannt geworden. Die zuständige Justizkommissarin Reding ist weiterhin nicht einverstanden damit, dass v. a. durch Pensionierungsregelungen die Möglichkeit eröffnet wird, dass die Justiz politisch gesäubert wird. Die Kommission beantragte in der Sache beim Gerichtshof ein Eilverfahren und forderte Ungarn auf, das strittige Gesetz bis zum Urteil nicht anzuwenden. Obwohl die Kommission zuvor geprüft hatte, ob das heftig umstrittene neue ungarische Mediengesetz nicht auch gegen europäisches Recht verstößt, hat sie hier keine Schritte unternommen.

Beim Datenschutz klagte die Kommission wegen der Entlassung des früheren Datenschutzbeauftragten, die mit der Neugründung der ungarischen Datenschutzbehörde einherging.

Der bisherige Amtsinhaber war von Orbán zum Rücktritt gezwungen worden. Die künftigen Datenschützer können nach einem neuen Gesetz aus „willkürlichen Gründen“, so eine Bewertung der EU-Kommission, entlassen werden. Das sei ein Verstoß gegen den Schutz vor vorzeitiger Amtsenthebung, eine Kernvorschrift des EU-Rechts, sowie gegen die EU-Charta der Grundrechte (Busse www.faz.net 25.04.2012; Winter SZ 25.04.2012, 9).

USA

Nackter Protest gegen Nacktscanner

Ein US-Amerikaner hat sich aus Protest gegen Sicherheitsscanner auf Flughäfen auf dem internationalen Airport im US-Bundesstaat Oregon komplett ausgezogen. Der 49jährige lief am 17.04.2012 nackt durch die Sicherheitskontrolle. Einige Fluggäste haben, so die Presse, sich und ihren Kindern die Augen zugehalten. Andere hätten gelacht und Fotos gemacht. Teile des Sicherheitsbereichs wurden vorübergehend geschlossen. Nach Polizeiangaben wurde der Mann wegen unzüchtiger Entblößung und ungebührlichem Verhalten festgenommen. Er erklärte, er sei Vielflieger und habe sich aus Protest gegen die als Belästigung empfundenen Körperscanner ausgezogen (SZ 19.04.2012, 9).

USA

Obama kündigt Sanktionen wegen Überwachungstechnologieexport an

Die USA wollen künftig gegen ausländische Behörden, Unternehmen und Personen vorgehen, die mit Satellitentechnologie und Internetkontrollen diktatorische Regime bei der Unterdrückung ihrer Bevölkerung unterstützen. Diese Politik zur Verhinderung staatlicher verordneter Verbrechen sei eine direkte Lehre aus dem von Nazi-Deutschland verantworteten Massenmord, erklärte US-Präsident Barack Obama in einer Rede im Holocaust-Museum in Washington. Eine am 23.04.2012 veröffentlichte präsidentielle Verordnung gegen Helfeshelfer der Regierungen in Syrien und Iran richtet sich konkret gegen den syrischen Geheimdienst, das syrische Telefonunternehmen Syriatel, das iranische Kommunikationsunternehmen Datak Telecom, Teherans Revolutionäre Garden, Irans Geheimdienst-Ministerium sowie generell die iranischen Sicherheitskräfte. Die Verordnung verbietet US-BürgerInnen und amerikanischen Banken auch Finanztransaktionen mit den genannten Organisationen. Gegen den Chef des syrischen Geheimdienstes Ali Mamluk verhängte die Verordnung ein Visa- und Einreiseverbot.

Obama erklärte, die Maßnahmen sollen helfen, dass moderne Kommunikationstechnologien und soziale Medien „die Bürger ermächtigen“ und nicht zu ihrer Unterdrückung dienen. Das syrische Regime nutze die Kontrolle von Internetforen, um Oppositionelle aufzuspüren. Es gibt Hinweise, dass Damaskus gezielt ausländische JournalistInnen durch das Abhören der Satellitentelefone überwacht. Nach Luftangriffen war anschließend die bekannte US-Kriegsreporterin Marie Coven getötet worden. Obama steht innenpolitisch unter Druck, die Opposition gegen das Assad-Regime besser zu unterstützen, z. B. durch Waffenlieferungen. Obama betonte, die Verhinderung von Massenmord in der Welt sei für seine Regierung „kein Nachklapp oder Nebensache“. Die US-Geheimdienste sollten in ihren Lage-Analysen künftig regelmäßig die Gefahren systematischen Gewaltmissbrauchs erfassen. Ein neues Gremium zur Entwicklung von Politiken gegen Gräueltaten wurde unter Leitung von Semantha Power, einer früheren langjährigen Menschenrechtsaktivistin, die 2011 massiv auf eine US-Intervention in Libyen gedrängt hatte, eingerichtet.

Derweil reist Alec Ross, der für digitale Diplomatie zuständige Berater der US-Außenministerin Hillary Clinton, um die Welt, um der digitalen Industrie begreiflich zu machen, dass die USA stellvertretend für den Westen eindeutige Interessen haben, wenn es darum geht, Schwellen- und Entwicklungsländer in die globalen Kommunikationsnetze einzubinden. Die USA würden alles unternehmen, um Meinungsfreiheit und damit Demokratie weltweit möglich zu machen. Konzerne wie Facebook und Google, deren soziale Netze eine zentrale Funktion bei der Vernetzung der Internetnutzenden erfüllen, haben längst langfristige Strategien für die Durchdringung der Märkte in den Ländern mit starker informationstechnischer Entwicklung. Dabei ergeben sich zwangsläufig Konflikte mit den von Obama formulierten Ansprüchen bzw. allgemein zwischen Wirtschaft und Politik (Wernicke SZ 24.04.2012, 8; Kreye SZ 25.04.2012, 4).

USA

W-LAN-Scan bei Google Street View erfolgte vorsätzlich

Als Google Kamera-Autos ausschickte, um für seinen Bilderdienst Street View die Straßen in aller Welt abzulichten, wurden nicht nur Fotostrecken erstellt. Vielmehr lokalisierten die Fahrzeuge auch WLAN-Hotspots und schnitten dabei nebenbei auch sonstige Dateninhalte mit, bis hin zu ganzen E-Mails, Web-Adressen und Passwörtern. Als die Angelegenheit 2010 im Rahmen der Überprüfung des hamburgischen Datenschutzbeauftragten (HmbBfDI) herauskam, war die Aufregung groß. Die US-amerikanische Telekommunikationsbehörde, die FCC (Federal Communications Commission), begann Untersuchungen über etwaige Rechtsverstöße Googles. Der Konzern erklärte die Datenpanne mit einem Versehen. Das Unternehmen verwies damals darauf, dass es die Position von WLAN-Routern erfasse, um diesen später, wenn sie Street View nutzen sollten, eine genaue Ortung zu ermöglichen. Später behauptete das Unternehmen, dass es wegen eines Softwarefehlers auch weitere Daten gesammelt, diese jedoch nie verwendet habe. Bei einer genaueren Überprüfung stellte sich heraus, dass u. a. E-Mails und Passwörter in den erfassten Datensplittern enthalten waren. Besonders groß scheint die „Beschämung“, von der der Konzern damals sprach, aber nicht gewesen zu sein.

Gering war auch die Bereitschaft, an der Untersuchung mitzuwirken.

Nach anderthalb Jahren im April 2012 veröffentlichte die FCC einen 25-seitigen Zwischenbericht. Die FCC-Untersuchung bestätigt nun, dass Googles Fahrzeuge von Mai 2007 an drei Jahre lang die Daten gesammelt haben. Aus dem Bericht ist deutlich die Frustration der Beamten über Googles Kooperation erkennbar. Das Unternehmen habe sich wiederholt geweigert, E-Mails und weitere Informationen herauszugeben. Auch die Namen der an den Vorfällen beteiligten Mitarbeitenden seien zurückgehalten worden: „Obwohl weltweit führend im Bereich der digitalen Suche, hat Google die Haltung eingenommen, dass die Suche nach den Namen seiner Angestellten ‚eine zu zeitaufwendige und beschwerliche Aufgabe sei'". Auf das Ersuchen nach Offenlegung der für das Projekt Verantwortlichen habe Google sogar einseitig festgelegt, dies würde ‚keinem nützlichen Zweck dienen'".

Schließlich erklärten die genervten Behördenverantwortlichen, Google habe seine Ermittlungen „absichtlich behindert und verzögert" und belegten das Unternehmen mit einer Geldbuße in Höhe von 25.000 Dollar. Zwar verdient der Konzern an einem einzigen Tag das Hundertfache dieser Summe am Tag. Doch ist die Summe die höchste, die die FCC mit einem Bußgeld verlangen kann. Die FCC stellte jedoch auch fest, dass die Street-View-Datensammlungen an sich nicht illegal gewesen, weil die Daten nicht verschlüsselt worden seien. Eine Konzernsprecherin teilte am Samstag mit: „Wir haben in gutem Glauben daran gearbeitet, um die Fragen der FCC während der ganzen Untersuchung zu beantworten; wir freuen uns, dass sie zum Ergebnis gekommen sind, dass wir uns im Einklang mit dem Gesetz befinden."

Wenig später wurde bekannt, dass der bislang unbenannte Google-Mitarbeiter, der laut FCC im Alleingang dafür gesorgt haben soll, dass Googles Street-View-Autos die unverschlüsselten WLANs angezapft haben, identifiziert ist. Es handelt sich um Marius Milner, der vor rund zehn Jahren mit seinem WLAN-Scanner NetStumbler eines der beliebtesten WarDriving-Tools entwickelt hatte. Milner habe bereits seit 2003 bei Google gearbeitet und sei seit 2008 im YouTube-Team tätig. Die Software für die Street-View-Autos, die laut der FCC-Untersuchung intern als „gstumbler" bezeichnet wird, soll Milner in den 20 Prozent seiner Arbeitszeit geschrieben haben, die Google-Mitarbeitenden für eigene Projekte zur Verfügung stehen. Das Ziel sei gewesen, die gesammelten Daten für andere Google-Projekte zu benutzen.

Gstumbler hat in der Zeit von 2007 bis 2010 unter anderem Suchabfragen und Mails in ungeschützten WLANs mitgeschnitten. Nach wie vor herrscht Unklarheit darüber, wer von den Plänen Milners wusste. Laut der FCC-Untersuchung hatte Milner seinen Arbeitgeber vorab über sein Vorhaben informiert. Er soll 2006 eine E-Mail an das gesamte Street-View-Team geschickt haben, in dem er seine Pläne erläuterte. In mindestens einem Fall soll er sich die gesammelten Daten angesehen haben, um nach besuchten Websites Ausschau zu halten. Erst als ein Mitarbeiter des Suchmaschinen-Bereichs gesagt habe, solche Daten hätten für Google keinen Wert, habe Milner sein Unterfangen nicht weiter verfolgt. Die Street-View-Manager bestreiten, von den Plänen gewusst zu haben. Insgesamt sollen laut der FCC sieben Google-Techniker an der Street-View-Software gearbeitet haben, einer davon soll den Code sogar Zeile für Zeile überprüft haben. Milner selbst verweigerte die Aussage.

Die Vizechefin der EU-Kommission und Justizkommissarin Viviane Reding reagierte auf den Bericht der FCC gereizt: „Ich habe den Eindruck, dass die Verantwortlichen von Google in diesem Fall das europäische Datenschutzrecht mit Füßen treten." Reding spricht von einem „planmäßigen Sammeln von WiFi-Daten ohne Kenntnis und Einwilligung der Bürger". Dies wecke „schlimmste Erinnerungen an einen orwellschen Überwachungsapparat". Jacob Kohnstamm, niederländischer Datenschutzbeauftragter und Vorsitzender der Artikel-29-Arbeitsgruppe der europäischen Datenschutzbehörden forderte eine globale Reaktion auf die FCC-Erkenntnisse. Google müsse zur Verantwortung gezogen werden. Alle Verfahren außer zweien in Deutschland wurden nach der Behauptung, hier habe es sich um ein Versehen gehandelt, eingestellt. In Hamburg sind weiterhin ein Aufsichtsverfahren und ein Strafverfahren anhängig. Der HmbBfDI Johannes Caspar meinte: „Jetzt erfahren wir, dass hier kein Fehler vorlag und dass die Leute im Unternehmen wussten, dass diese Daten gesammelt wurden. Das bringt die Sache in ein völlig neues Licht." Seine Behörde ermittelt in dem Fall weiter

(www.spiegel.de 16.04.2012; SZ 17.04. 2012, 21; www.heise.de 02.05.2012; O´Brien www.nytimes.com 02.05.2012; Der Spiegel 19/2012, 18).

USA

Volkszählungsdaten 1940 im Netz

Mehr als 3 Jahre lang haben Archivare des National Archive in den USA daran gearbeitet, die Daten der dortigen Volkszählung aus dem Jahr 1940 zu digitalisieren. Diese Daten sind seit dem 02.04.2012 im Netz verfügbar und können durchsucht und heruntergeladen werden. Nutzungsbeschränkungen gibt es keine. Die Befragung wurde damals insbesondere durchgeführt um zu ermitteln, wie viele Sitze die einzelnen amerikanischen Bundesstaaten im Kongress zu beanspruchen haben, da sich diese Zahl nach der Bevölkerung richtet. Außerdem sollte dabei überprüft werden, wie korrekt die Geburtsregister geführt werden. Neben den Befragungen wurden dazu auch die Registerkarten ausgewertet – die dabei gewonnenen Daten sind allerdings nicht erhalten geblieben. Auch ohne diese ist der Datenschatz gewaltig. Insgesamt 3,8 Millionen auf Mikrofilm gespeicherte Fotos mit den Fragebögen von mehr als 20 Millionen Menschen wurden gesichtet und aufbereitet. In diesen Bögen fragten die „Enumerators", die Volkszählenden, nicht nur nach Standardinformationen wie Name, Alter, Geschlecht, Hautfarbe, Bildung und Geburtsort. Sie wollten auch wissen, wie hoch das wöchentliche Einkommen des Befragten war, wo ihre Eltern geboren wurden und bei Frauen, wie oft sie verheiratet waren. Die Frage nach dem Einkommen sorgte damals für hef-

tige Debatten und ein republikanischer Senator versuchte, sie aus dem Bogen streichen zu lassen. Dies blieb ohne Erfolg, doch konnten die Befragten die Antwort verweigern, wenn sie das wollten – es wollten nur 2%.

Das Nationalarchiv schreibt in der Ankündigung auf seiner Website, dass die Daten einen historisch interessanten Einblick in die Zeit der großen Depression geben. Sie erzählen das Leben von 132 Millionen AmerikanerInnen, in einer Zeit, als das Land sich durch Wirtschaftskrise und Weltkrieg wandelte. Die Suche ist allerdings etwas mühsam. Die Informationen sind nach den Befragungsbezirken von damals verschlagwortet. Wer also seinen Großvater sucht, muss wissen, wo er damals wohnte und dann auf bereitgestellten Karten nachschauen, in welchem Befragungscluster (enumeration district) diese Adresse lag. Ein Personenindex ist in Arbeit, aber noch nicht fertig. Er soll in 6 bis 9 Monaten verfügbar sein (Biermann http://blog.zeit.de 02.04.2012).

USA

FBI-Geschichte veröffentlicht

Bestseller-Autor Tim Weiner hat ein Buch über das Federal Bureau of Investigation und dessen früheren Chef J. Edgar Hoover geschrieben (FBI - Die wahre Geschichte einer legendären Organisation, S. Fischer Verlag, Frankfurt a. M., 704 S., 22,99 Euro). Gemäß der Darstellung des Autoren war das FBI, also die US-amerikanische Bundespolizei, von ihrer Gründung vor 103 Jahren an vor allem ein Machtinstrument der jeweiligen Präsidenten, die sich in einem Krieg wähnten. In diesen Kriegen war das FBI ein Werkzeug zum Spionieren, Intrigieren und zum Machterhalt. Rechtsstaatlichkeit spielte eine untergeordnete Rolle. Wie kein anderer verkörperte J. Edgar Hoover die Behörde, die er 48 Jahre lang leitete. Weiner beschreibt, dass dieser über jede und jeden eine Akte anlegte: „Hoover diente nicht dem Gesetz, er war das Gesetz. Präsident Truman warf ihm 1945 sogar vor, eine amerikanische Gestapo aufzubauen. Doch kein Präsident hatte den Mut, Hoover zu entlassen."

Nach den Anschlägen vom 11.09.2012 startete das FBI eines der größten Überwachungsprogramme der Geschichte. Die Bush-Regierung forderte immer mehr Überwachung, bis im März 2004 FBI-Chef Robert Mueller sich mit Bedenken an Justizminister Ashcroft wendete, was Weiner beschreibt: „In der gleichen Nacht wurde Ashcroft wegen einer lebensgefährlichen Entzündung der Bauchspeicheldrüse notoperiert. Weil Bush das Programm aber unbedingt verlängern wollte, entsandte das Weiße Haus eine Delegation auf die Intensivstation, um Ashcrofts Unterschrift einzuholen. Als Mueller das hörte, fuhr er ebenfalls hin. Bushs Abgesandte standen schon am Bett des Ministers, aber Ashcroft lehnte ab. Es war eine Szene wie in einem Mafia-Film." Nach Einschätzung des Autors hat sich seit der Wahl von Obama beim FBI einiges zum Guten verändert. Erstmals in der FBI-Geschichte könne man davon sprechen, dass sich Freiheit und Sicherheit in einer Balance befinden (Der Spiegel 11/2012, 88).

USA/China

Romney profitiert von chinesischer Videoüberwachungstechnik

Bain Capital ist eine von Mitt Romney, dem republikanischen Kandidaten für die US-Präsidentschaftwahl Ende 2012 gegründete Kapitalgesellschaft. Bain Capital kaufte im Dezember 2011 die Videoüberwachungsabteilung des chinesischen Unternehmens Uniview Technologies, das für sich in Anspruch nimmt, der größte Lieferant für das Regierungs-"Programm sichere Städte" zu sein. Das Programm ermöglicht es, Behörden, Universitäten, Krankenhäuser, Moscheen und Kinos über Überwachungszentralen zu beobachten. Uniview Technology produziert Infrarot-Aufstandsbekämpfungskameras und Software, die es Polizeibehörden ermöglicht, Bilder in Echtzeit über das Internet auszutauschen. Zu den Projekten gehörte eine Notfallüberwachungszentrale im Tibet, die eine „solide Basis schafft für die Aufrechterhaltung sozialer Sicherehit und für den Schutz eines friedlichen Lebens für die Bevölkerung", so die Webseite von Uniview.

Der tibetianische Mönch Loksag aus der Provinz Gansu teilte mit, dass das Kamerasystem den Behörden die Identifizierung und Verhaftung von 200 Mönchen ermöglichte, die sich 2008 am Protest in seinem Mönchskloster beteiligten: „In unserem Kloster sind überall Videokameras, deren einziger Zweck es ist, uns Angst einzujagen." R. Bradford Malt, Manager der Investment-Gesellschaft von M. Romney, stellte klar, dass dieser seine Einlagen tätigte, bevor Uniview gekauft wurde und dass er keine Rolle bei dem Engagement gespielt habe. Romney habe keine Kontrolle über die Investitionen des asiatischen Fonds gehabt. Gemäß Romneys eigenen Angaben von August 2011 verdienten er und seine Frau mindestens 5,6 Mio. Dollar durch die stillen bzw. Renten-Anteile an Bain.

Romney forderte im Rahmen der seiner politischen Kampagne eine harte Linie gegen die Unterdrückung von Religionsfreiheit und politischer Opposition durch die chinesische Regierung. Kritiker meinten, dass Bains Erwerb von Uniview zumindest gegen den Geist der US-Sanktionen gegen Peking verstoßen, die nach der Unterdrückung der Proteste auf dem Tienanmen-Platz im Jahr 1989 erlassen wurden. Diese verbieten US-Unternehmen den Export von Produkten zur „Kriminalitätskontrolle" an China, z. B. Fingerabdruckssysteme, Fotoidentifikation oder Nachtsichtgeräte. Die meisten Videotechnologien werden aber von den Sanktionen nicht explizit erfasst. Kanadische Menschenrechtsgruppen fanden 2001 heraus, dass chinesische Sicherheitsbehörden westliche Videotechnologie zur Identifikation von Protestierenden auf dem Tienanmen-Platz nutzten. Im Rahmen seiner Kampagne beschuldigte Romney die Obama-Administration in Bezug auf China, wirtschaftliche Interessen über die Menschenrechte zu stellen. In jüngerer Zeit waren westliche Unternehmen dafür kritisiert worden, dass sie der chinesischen Regierung ausgeklügelte Überwachungstechnologie verkauft haben. Genannt wurden u. a. Honeywell,

General Electric, IBM und United Technologies. 2007 konnte Yahoo ein Klageverfahren gegen sich nur dadurch abwenden, dass es zugab, den Behörden E-Mails eines Journalisten ausgeliefert zu haben, der danach zu einer 10jährigen Freiheitsstrafe wegen der Verletzung von Staatsgeheimnissen verurteilt wurde.

Bain verteidigte den Kauf von Uniview damit, dass seine Produkte der Kriminalitätsvorbeugung und nicht der politischen Unterdrückung dienten. Uniview verweist stolz auf seine engen Verbindungen zu chinesischen Sicherheitskreisen und brüstet sich damit, die regionalen Sicherheitsbehörden mit seinen Überwachungssystemen zu unterstützen: „Soziales Management und gesellschaftlicher Aufbau machen neue Überwachungs- und Kontrollsysteme nötig.“ Vorstandschef Zhang Pengguo wird in einer Werbebroschüre wie folgt zitiert: „Eine harmonische Gesellschaft ist die wesentliche Eigenschaft des Sozialismus mit chinesischem Anlitz.“

Chinesische Städte investieren stark in Überwachungstechnologie. Chonqing in der Provinz Sechuan gibt gemäß staatlichen Medien 4,2 Milliarden Dollar für ein Netzwerk von 500.000 Kameras aus. Die Provinz Guangdong, das an Hongkong angrenzende Industriezentrum, installiert 1 Million Kameras. In Peking versucht die städtische Regierung Kameras in allen Vergnügungsvierteln zu installieren, zusätzlich zu den 300.000 Kameras, die anlässlich der Olympiade 2008 aufgebaut wurden. Nach Aussagen von Nicholas Bequelin, einem Forscher bei Human Rights Watch Hongkong, versucht die Regierung durch die Verbindung von Internet, Mobilkommunikation und Videoüberwachung ein allgegenwärtiges Kontrollsystem aufzubauen: „In Sachen Überwachung ist China bezüglich seiner totalitären Bestrebungen äußerst offenherzig“.

Yang Weidong, ein politisch aktiver Filmemacher, sagte, dass ein Phalanx von 13 Kameras in und um sein Wohnhaus eingerichtet wurden, nachdem er eine Interview-Bitte an Präsident Hu Jintoa geäußert und damit den Zorn der örtlichen Sicherheitskräfte auf sich gerichtet hatte. Im Januar 2012 wurde der Künstler Ai Weiwei von der Polizei einvernommen, nachdem er Steine auf Kameras geworfen hatte, die auf seine Eingangstür ausgerichtet sind. Die 45jährige Menschenrechtsanwältin Li Tiantian aus Shanghai berichtete, dass die Polizei im Eingangsbereich eines Hotels erstelltes Filmmaterial benutzte, um sie während einer dreimonatigen illegalen Inhaftierung im Jahr 2011 unter Druck zu setzen. Das Video zeigte sie in Begleitung mit anderen Männern. Während den Befragungen hätte die Polizei sie wegen ihres Sexuallebens verhöhnt und gedroht, das Video ihrem Freund zu zeigen. Dieser habe sich jedoch geweigert, das anzuschauen: „Die Schwere des Eindringens in das Privatleben der Menschen ist schlimmer als je zuvor. Ich fühle mich verletzlich, weil ich weiß, dass die Polizei mich permanent beobachtet“ (Andrew Jacobs u. Penn Bullock, When Technology Intrudes, The New York Times, Articles selected for Süddeutsche Zeitung, 26.03.2012, 1).

China

Entmachteter Bo Xilai soll Parteifunktionäre abgehört haben

Aus der Affäre um den geschassten chinesischen Politstar Bo Xilai wurde ein Abhörskandal für Chinas Kommunistische Partei. Bo Xilai soll nach US-amerikanischen Presseberichten reihenweise hochrangige Politiker abgehört haben - bis hin zu Staatschef Hu Jintao. Die Affäre um Bo Xilai war zunächst eine Räuberpistole um Mord, Erfolg und Absturz. Nun wurde bekannt, dass der jüngst suspendierte Politiker seine Konkurrenten in großem Stil bespitzeln ließ. Rund ein Dutzend anonyme Informanten mit besten Verbindungen in Parteikreise haben demnach bestätigt, dass Bo Xilai über Jahre hinweg die Telefongespräche von Politikern mitgeschnitten haben, wenn diese Chongqing besuchten. Die Metropole mit 30 Millionen EinwohnerInnen, in der Bo als Parteichef waltete, gilt als kommende Boom-Region; entsprechend regelmäßig waren die Visiten.

In der offiziellen Begründung für den Sturz des aufstrebenden Politstars fehlt der Spionageaspekt bisher komplett. Der vage Vorwurf lautet „schwere Disziplinarvergehen“. Ins Detail geht die Partei nicht, diese Formulierung wird in China aber in der Regel im Zusammenhang mit Korruptionsdelikten verwendet. Gegen seine Frau, Gu Kailai, wird wegen der Ermordung eines britischen Geschäftsmanns ermittelt. Gemäß westlichen Presseberichten finden die Abhörpraktiken in internen Papieren Erwähnung. Die gewonnenen Informationen nutzte Bo dem gemäß gezielt, um seinen eigenen Aufstieg in der Partei voranzutreiben. „Er wollte ganz genau wissen, welche Führer ihm wohl gesonnen waren und welche nicht“, so die New York Times. Das Personal von Staatspräsident Hu Jintao habe allerdings im August 2011 die Abhörmaßnahme bemerkt. Bo soll in der Millionenstadt ein Netzwerk aus Wanzen und Abhöreinrichtungen für Telefone installiert haben. Dabei stand offiziell der Kampf gegen das organisierte Verbrechen im Vordergrund. Parallel sei das Netz allerdings auch für Bos persönliche Karriereplanung genutzt worden.

Der charismatische Bo Xilai wurde lange Zeit als einer der Hoffnungsträger der Partei angesehen. Noch im Jahr 2012 war erwartet worden, dass er in den ständigen Ausschuss des Politbüros aufsteigt. Bo verkörperte einen linkskonservativen Kurs, der im Widerspruch zum wachstumsorientierten Kurs der restlichen Parteiführung stand. So versprach er als Parteichef von Chongqing die Unterschiede zwischen Arm und Reich einzuebnen. Zum Verhängnis wurde Bo unter anderem die Affäre um den Polizeichef von Chongqing, Wang Lijun. Dieser hatte Bo lange als rechte Hand im Kampf gegen die Korruption gedient, war Anfang Februar 2012 jedoch entlassen worden. Daraufhin war der Polizist in das US-Konsulat in Chengdu geflüchtet. Angeblich soll Wang Lijun um sein Leben gefürchtet und Asyl gesucht haben. Nach einem Tag begab er sich nach US-Angaben freiwillig in die Obhut der Pekinger Zentralregierung. Wang soll im Besitz von Belastungsmaterial gegen seinen früheren Chef Bo sein, den er als „größten Mafia-Boss“ beschrieben haben soll (www.spiegel.de 26.04.2012; SZ 27.04.2012, 8).

Technik-Nachrichten

Nokia lässt Haut bei Anrufe leuchten und vibrieren

Der finnische Handy-Hersteller Nokia hat in den USA ein Patent für Vibrations-Tatoos beantragt, mit denen KundInnen auf eingehende Anrufe aufmerksam gemacht werden sollen. Die Idee ist, dass das Handy elektromagnetische Wellen aussendet, wenn beim Telefon ein Anruf eingeht, eine SMS ankommt oder die Batterie aufgeladen werden muss. Durch den Impuls soll ein mit spezieller magnetischer Farbe tätowiertes Bild auf der Haut sichtbar werden und vibrieren (SZ 23.03.2012, 22).

Datenschutzfreundlicher Facebook-Assistent

Ixquick, der datenschutzfreundliche Betreiber der Suchdienste Ixquick (http://www.ixquick.com) und Startpage (http://www.startpage.com) hat für die Fanseite auf Facebook einen Assistenten programmiert. Diese Anwendung soll das Bewusstsein für mehr Privatsphäre wecken und gleichzeitig helfen, die eigenen Einstellungen auf Facebook unter Datenschutzgesichtspunkten zu perfektionieren.

Die App kann ohne Auflagen geladen werden und kommt ohne das Sammeln von Daten aus. Ixquick verzichtet auf Facebook Connect. Auch bei der Datenübertragung (Nutzung des Assistenten) wird auf Sicherheit durch Etablierung einer SSL-Verbindung gesetzt.

Rechtsprechung

BVerwG

Kein Verbot für Fotos von Polizeieinsätzen

Nach einem Urteil des Bundesverwaltungsgerichts (BVerwG) vom 28.03.2012 darf die Polizei JournalistInnen das Fotografieren von deren Einsatz nicht einfach verbieten (AZ: 6 C 12.11). Hintergrund war der Einsatz eines Sondereinsatzkommandos (SEK) im März 2007 in der Fußgängerzone von Schwäbisch Hall. Acht Beamte hatten ein mutmaßliches Mitglied der russischen Mafia zum Augenarzt gebracht. Der Einsatzleiter verbot zwei Lokaljournalisten Fotoaufnahmen mit der Begründung, die Anonymität der Beamten müsse gesichert werden. Der Zeitungsverlag Schwäbisch Hall, der das Haller Tagblatt herausgibt, sah darin eine unzulässige Beeinträchtigung der Pressefreiheit, reichte Klage ein und bekam in dritter Instanz Recht. In erster Instanz wurde die Klage am Verwaltungsgericht Stuttgart abgewiesen. Beim Verwaltungsgerichtshof in Mannheim bekamen die Journalisten dagegen Recht. Die Revision des Landes te einer der beiden Männer, die wegen des Mordes an dem Schauspieler verurteilt worden waren, dagegen geklagt, dass sein Name in einem Artikel auf einer österreichischen Webseite veröffentlicht wurde. Die beiden Mörder haben rund ein Dutzend Prozesse geführt, um ihre Namen aus Online-Archiven tilgen zu lassen. Der BGH urteilte, das Recht des Webseiten-Betreibers auf freie Meinungsäußerung habe Vorrang vor dem Persönlichkeitsschutz. Der Fall sei nach deutschem Recht zu entscheiden, weil der Kläger in Deutschland wohne; eine mögliche Beeinträchtigung seines Ansehens durch die Veröffentlichung trete deshalb vor allem in Deutschland ein. Der BGH hatte den Fall zunächst dem Europäischen Gerichtshof in Luxemburg vorgelegt, um unter anderem die Zuständigkeit nach EU-Recht klären zu lassen (vgl. DANA 4/2011, 184).

Bereits 2009 hatte der BGH entschieden, dass Meldungen, in denen der Kläger mit Namen genannt wurde, weiterhin in einem Online-Archiv zum Abruf bereitgehalten werden dürfen. Damals hatte der BGH betont, es bestehe ein anerkennenswertes Interesse der Öffentlichkeit daran, auch vergangene zeitgeschichtliche Ereignisse zu recherchieren. Der Anwalt des Klägers hatte in der Verhandlung argumentiert, dieser habe „keine Chance auf Resozialisierung“, wenn er ständig wieder mit der Tat konfrontiert werde. Der Anwalt des Webseiten-Betreibers hielt dagegen: Eine Pflicht zur Löschung alter Artikel über zeitgeschichtliche Ereignisse führe dazu, „dass Geschichte getilgt wird.“ Der BGH betonte, dass mit wachsender zeitlicher Distanz die Bedeutung des Resozialisierungsinteresses des Straftäters zunehme. Ob das „Resozialisierungsinteresse“ beeinträchtigt ist, hängt schon nach einer früheren BGH-Entscheidung allerdings auch davon ab, wie gravierend der Eingriff ist. In einem Online-Archiv sei die Reichweite einer Meldung so gering, dass die Wiedereingliederung entlassener Straftäter nicht nennenswert beeinträchtigt wird. Ganz erfolglos scheint die Klageserie der beiden Mörder trotz vieler negativen letztinstanzlichen Entscheidung nicht gewesen zu sein: Wer nach deren Namen sucht, findet sie zumindest nicht auf der ersten Google-Trefferliste (www.heise.de 09.05.2012; SZ 09.05.2012, 15).

Baden-Württemberg gegen dieses Urteil wiesen die Leipziger Richter zurück.

Das BVerwG entschied, dass ein SEK-Einsatz ein zeitgeschichtliches Ereignis sei, von dem Bilder auch ohne Einwilligung der BeamtInnen gemacht werden dürften. Zwar hätten die PolizistInnen einen Schutz-Anspruch. Zur Abwendung von Gefahren „bedarf es aber regelmäßig keines Verbots der Anfertigung von Fotografien, wenn zwischen der Anfertigung der Fotografien und ihrer Veröffentlichung hinreichend Zeit besteht, den Standpunkt der Polizei auf andere, die Pressefreiheit stärker wahrende Weise durchzusetzen“.

Der Bundesverband Deutscher Zeitungsverleger (BDZV) begrüßte die Entscheidung „im Sinne der Pressefreiheit“. BDZV-Sprecherin Anja Pasquay sagte, es sei die gute und verantwortungsvolle Arbeit einer Zeitung genau abzuwägen, ob Fotos veröffentlicht werden können: „Aber von vornherein zu sagen, man dürfe nicht fotografieren, das ging aus unserer Sicht zu weit.“ Der BDZV hatte vor der Verhandlung erklärt, gedruckte und elektronische Medien wären in ihrer durch das Grundgesetz gewährten Freiheit eingeschränkt, wenn sich die Rechtsauffassung des Landes durchsetzt (www.rhein-zeitung.de 28.03.2012; SZ 29.03.2012, 17).

BGH

Kein Anspruch auf Tilgung aus Online-Pressearchiven

In einem Urteil vom 08.05.2012 entschied der Bundesgerichtshof (BGH) über die Klage gegen einen österreichischen Webseiten-Betreiber, dass einer der beiden verurteilten Mörder des Schauspielers Walter Sedlmayr weiterhin in Online-Archiven mit Namen genannt werden darf (Az. VI ZR 217/08). Der BGH bestätigte damit frühere Urteile (DANA 1/2010, 43). Deutsche Gerichte sind nach der Entscheidung auch für Klagen gegen Veröffentlichungen auf Webseiten aus anderen EU-Staaten zuständig, sofern der Betroffene den Mittelpunkt seiner Interessen in Deutschland hat. Im konkreten Fall hat-

BSG

Jobcenter-Anfragen bei Dritten nicht ohne vorherige Befragung der Betroffenen

Gemäß einem Urteil des Bundessozialgerichts (BSG) vom 25.01.2012 ist ein Jobcenter dazu verpflichtet, in jedem Fall die schutzwürdigen Interessen von Leistungsempfängern zu beachten und vor einer Kontaktaufnahme mit Dritten zunächst das Einverständnis der Leistungsempfänger einzuholen (Az. B 14 AS 65/11 R). Nach den auch für das Sozialgesetzbuch (SGB) II geltenden datenschutzrechtlichen Vorschriften hat jeder Anspruch darauf, dass die ihn betreffenden Sozialdaten von den Leistungsträgern nicht unbefugt erhoben, verarbeitet oder genutzt werden.

Die Kläger des zugrunde liegenden Streitfalls machten eine Verletzung datenschutzrechtlicher Regelungen durch das beklagte Jobcenter geltend. Das 1957 und 1966 geborene Ehepaar, das Arbeitslosengeld II bezieht, bewohnte zusammen mit mehreren Kindern und weiteren Familienangehörigen bis Ende Februar 2008 ein Haus. Das Mietverhältnis wurde von der Vermieterin, vertreten durch den Haus- und Grundbesitzerverein, gekündigt. Die Kläger hatten hierfür eine von ihnen selbst aufgebrachte Kaution in Höhe von 2.611,78 Euro hinterlegt. Im Dezember 2007 unterzeichneten sie einen Mietvertrag für ein anderes Haus. Bei Beginn des Mietverhältnisses im Februar 2008 forderte der Vermieter eine Mietkaution in Höhe von 1.700 Euro. Den Antrag der Kläger, die Mietkaution darlehensweise zu übernehmen, lehnte das beklagte Jobcenter ab und verwies auf die Mietkaution für das bislang bewohnte Haus, die zur Begleichung der neuen Kaution eingesetzt werden könne. Die Kläger machten geltend, die hinterlegte Mietkaution für das bislang bewohnte Haus stehe voraussichtlich erst mit Ablauf der sechsmonatigen Prüfungsfrist der Vermieterin und daher weit nach Fälligkeit der Mietkaution für das neue Haus zur Verfügung. Daraufhin wandte sich das Jobcenter wegen der Auszahlung der Kaution an den Haus- und Grundbesitzerverein unter dem Betreff „Leistungen nach dem SGB II im Mietverhältnis ...“ mit Angabe der bisherigen Adresse und des Namens der Kläger und bat unter anderem um Mitteilung des Auszahlungstermins und der Höhe der Kaution. In der Folgezeit telefonierten Bedienstete des Jobcenters mehrmals mit dem Haus- und Grundbesitzerverein und erkundigten sich nach dem Sachstand. Ende Februar 2008 beantragten die Kläger beim Jobcenter außerdem je einen Schrank für ihre Kinder, weil diese über keine Schränke verfügten, da in dem bisherigen Haus Einbauschränke gewesen seien. Am 19.03.2008 telefonierte ein Bediensteter des Jobcenters wegen dieser Angelegenheit mit dem Ehemann der früheren Vermieterin.

Im Rahmen ihrer auf die Bewilligung der Mietkaution gerichteten Klage machten die Kläger u. a. die Verletzung ihres Sozialdatenschutzes geltend. Erst durch das Schreiben des Jobcenters habe die Vermieterin von deren Leistungsbezug erfahren. Die Kläger seien nunmehr dem Hohn und Spott der Familie der ehemaligen Vermieterin ausgesetzt. Das Sozialgericht Freiburg hat den Antrag der Kläger, festzustellen, dass das Jobcenter durch sein Verhalten unbefugt Sozialgeheimnisse offenbart habe, abgewiesen. Das Landessozialgericht Baden-Württemberg wies die Berufung zurück. Mit der vom BSG zugelassenen Revision hatten die Kläger eine Verletzung von § 35 Abs. 1 SGB I und ihres Grundrechts auf informationelle Selbstbestimmung gerügt.

Das BSG stellt in seinem Urteil fest, dass das beklagte Jobcenter durch sein Schreiben an den Haus- und Grundbesitzerverein sowie durch seine Telefongespräche mit diesem und mit dem Ehemann der früheren Vermieterin der Kläger unbefugt Sozialgeheimnisse der Kläger offenbart hat, indem er den Leistungsbezug der Kläger mitgeteilt hat. Das Jobcenter kann das Offenbaren der Sozialdaten hier nicht damit rechtfertigen, dass dies erforderlich gewesen sei, um die eigenen Aufgaben zu erfüllen. Es musste in jedem Fall die schutzwürdigen Interessen der Kläger beachten und hätte deshalb vor einer Kontaktaufnahme mit Dritten zunächst das Einverständnis der Kläger einholen müssen (www.kostenlose-urteile.de 02.05.2012).

Buchbesprechung



Benedikt Buchner (Hrsg.),
Datenschutz im Gesundheitswesen – Grundlagenwissen - Praxislösungen - Entscheidungshilfen,
Loseblattsammlung, Grundwerk Januar 2012. AOK-Verlag Remagen.

(tw) Wenn etwas im Datenschutz weder für die betroffenen Menschen noch für Daten verarbeitende Stellen konsistent und verständlich ist, dann ist es das Regelwerk im Gesundheitswesen. Wenn nun ein Werk genau zu diesem Thema auf den Markt kommt, so sind die Erwartungen entsprechend hoch, verspricht sich doch die interessierte LeserIn Erkenntnisse über die vielen bestehenden schwarzen Flecken in der fachlichen Diskussion, z. B. über Regeln, die für die Gesundheitsämter gelten, die Behandlung und Unterbringung von psychisch Kranken, die absolut intransparente und verwirrend im SGB V geregelte Datenverarbeitung der Krankenkassen, die nicht leichter zu duchschauende Datenverarbeitung bei den privaten Krankenversicherungen, die Abrechnungsvermittlung durch die Kassenärztlichen Vereinigungen, die Apothekenrechenzentren, die Hausarztverbände oder die privatärztlichen und gewerblichen Verrechnungsstellen, die heiklen Kommunikationen beim Disease Management, bei der integrierten Versorgung und anderen datengetriebenen Versorgungsstrukturen, die völlig außerhalb des öffentlichen Fokus liegenden Datenauswertungen zum Zweck der Wirtschaftlichkeitskontrolle oder der Qualitätsprüfung, die medizinische Forschung, von der Eigenforschung von Ärzten bis hin zu Biobanken, Krankheitsregistern und Forschungsnetzwerken und nicht zuletzt die Datenzweitverwertung etwa durch die Pharmaindustrie, die derzeit zumindest in den Fachmedien skandalbegründet Aufmerksamkeit findet.

Das neue Werk befasst sich aber nicht mit diesen vielen Spezialfragen. Es zielt nicht auf die Überbrückung des rechtsdogmatischen Grabens zwischen MedizinrechtlerInnen und DatenschützerInnen und auf die erstmalige Ausfüllung der vielen schwarzen Flecken ab, sondern auf die Ausbildung von NeueinsteigerInnen beim Gesundheitsdatenschutz. Das als Einstiegs-Leitfaden von Datenschutzpraktikern für DatenschutzpraktikerInnen insbesondere in ambulanten Arztpraxen und Krankenhäusern, auch in Krankenkassen konzipierte Werk präsentiert im separaten – auch separat lesbaren – Kapiteln wichtige Grundbegriffe des Medizindatenschutzes. Insbesondere für neue betriebliche Datenschutzbeauftragte und für Datenschutz zuständige IT-Verantwortliche werden die Grundbegriffe eingeführt und erläutert. Dabei wird nach einer systematischen Einführung (Buchner) didaktisch aufbereitet jeweils ein Sachgebiet dargestellt: Aufgaben des betrieblichen/ behördlichen Datenschutzbeauftragten (Biewald), Vorgehensweise eines betrieblichen Datenschutzbeauftragten im Krankenhaus (Pampel/Biewald), IT-Organisation (Pampel), Krankenhausdatenschutz (Pampel), Einführung in den GKV-Datenschutz (Albers), Arztpraxis (Menzel), IT-Grundbegriffe und IT-Sicherheit (Maslo). Einige vorgesehene Kapitel sind noch unbesetzt, z. B. zu Rehabilitation und Teilhabe, zu Pflege, zum Beschäftigtendatenschutz.

Stil und Inhalte der Beiträge sind nicht einheitlich. Als Basis für die Grundausbildung eines Gesundheitsdatenschützers ist das Werk geeignet. Bei den Technikbeiträgen geht manchmal der Gesundheitsbezug verloren. Besondere Regelwerke zum IT- oder Datenschutzmanagement wie die Datenschutzverordnung von Schleswig-Holstein oder die aktuelle Orientierungshilfe der Datenschutzkonferenz zu Krankenhausinformationssystemen, werden (noch?) nicht referiert. Auf einer CD gibt es weitere elektronische Hilfen und Formulare. Ein Index erschließt das nicht sofort in seiner Grundstruktur erfassbare Gesamtwerk nach Stichworten. Das Literaturverzeichnis gibt einige wenige Hinweise für weitere Recherchen. Das Werk gibt einen Einblick für den EinsteigerInnen und für manchen Fortgeschrittenen. ExpertInnen finden aber wegen der nur spärlichen Literatur- und Rechtsprechungshinweise keine weiterführenden Hilfen. Durch den Loseblatt-Charakter kann das Werk kontinuierlich weiter ausgebaut und können die vorhandenen Beiträge aufeinander abgestimmt werden. Fazit: Für die PraktikerIn eine gute Hilfe, in besonderen Bedarfsfällen muss sie weitergehende Informationsquellen für ihre Tätigkeit heranziehen.


Sie bestimmen mit!
Es werden Themen zu der DANA-Ausgabe 4/2012 gesucht. Nennen Sie Ihre Wünsche. Wir kümmern uns um die Verwirklichung.
Natürlich sehen wir es sehr gerne, wenn Sie selbst ein wenig Arbeit beisteuern und einen Artikel schreiben.
Einsendeschluss für diese Aktion ist der 15. Oktober 2012.

Grenzenlose „Freiheit“ über den Wolken.



Amerikanische Regierungsbehörden können durch das vom Europäischen Parlament im April 2012 beschlossene transatlantische Abkommen zum Transfer von Flugpassagierdaten „frei“ auf folgende Datenfelder zugreifen:

• Datum, an dem der PNR erstmals angelegt wurde sowie nachfolgende Änderungen • Flugtag(e) und -strecke(n), so genannte Segmente • Flugnummer(n) • Flugzeiten (Angaben jeweils in Ortszeiten) • Flugdauer • Fluggerät (Typenbezeichnung des zum Einsatz kommenden Flugzeugs) • Buchungsklasse (jedem Flugtarif ordnet die Fluglinie eine Bezeichnung zu, um später auch den richtigen Tarif berechnen zu können).•. Vor- und Zuname des oder der Passagiere (es können mehrere Personen auf einem PNR gespeichert werden, sofern sie die gleichen Flugtage und -strecken fliegen) • Wohnadresse und Telefonnummer eines oder mehrere Passagiere • Adresse und Telefonnummer am Zielort, um bei Änderungen des Flugplans einen Passagier erreichen zu können • Zahlungsart z. B. eine Kreditkartennummer und Ablaufdatum der Kreditkarte • Rechnungsanschrift • Vielflieger-Eintrag (beschränkt auf abgeflogene Meilen und Anschrift(en)) • Name der Buchungsagentur (Reisebüro, IATA-Ausgabestelle, Firmenbuchungsstelle u. ä.) • Sachbearbeiter der Buchung • Codeshare-Information: wenn eine andere Fluggesellschaft als durch die Flugnummer angeführte den Flug ausführt • Reisestatus des Passagiers: welche Strecken bereits abgeflogen sind und welche er noch vor sich hat • Informationen über die Splittung/Teilung einer Buchung: wird nach dem erstmaligen Abschluss eines PNR ein oder mehrere Passagiere wieder davon getrennt, weil sie beispielsweise nun eine andere Strecke fliegen möchten, müssen nicht alle Daten neu eingegeben werden, sondern man „splittet“ (teilt) den PNR in einen Original-PNR und einen Split-PNR • E-Mail-Adresse • allgemeine Bemerkungen • Informationen über Flugscheinausstellung (Ticketing) • Daten über den Flugtarif • Daten der Flugscheinausstellung • Sitzplatzinformationen: welcher Status (auf Anfrage, bestätigt usw.) und dann die Sitzplatznummer • Nummern der Gepäckanhänger (baggage tags) • Historie über nicht angetretene Flüge (no show) • Fluggäste mit Flugschein, aber ohne Reservierung (go show) • spezielle Serviceanforderungen z. B. bezüglich Essen (koscher, vegetarisch u. a.), so genannte OSI- und SSI/SSR–(Sensitive Security Information/Special Service Requests) Elemente • Information über den Auftraggeber (received from) • alle Änderungen des PNR mit Datum, Uhrzeit und Aktion (PNR-History) • Zahl der Reisenden im PNR • etwaige APIS-Informationen (Advance Passenger Information System) • ATFQ-Felder (automatische Tarifabfrage) • ggf. alle zu einer Mietwagen- oder Hotelbuchung gehörenden Daten (Bonuskonten einzelner Hotel- oder Mietwagenketten etc.)